UNIVERSIDADE FEDERAL DE PERNAMBUCO
CENTRO DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELETRÔNICA E SISTEMAS

DECODIFICACAO PROBABILÍSTICA DE CÓDIGOS LINEARES

POR

RICARDO MENEZES CAMPELLO DE SOUZA

Depart.º de Eng.ª Eletrônica e Sistemas
Centro de Tecnologia
Cidade Universitária
50.000 Recife - PE

TESE DE MESTRADO

DECODIFICAÇAO PROBABILÍSTICA
DE
CÓDIGOS LINEARES

por

Ricardo Menezes Campello de Souza

DEPARTAMENTO DE FÍSICA

UNIVERSIDADE FEDERAL DE PERNAMBUCO

Cidade Universitária - Tel. 227.0871

RECIFE - BRASIL

- 1979 -

UNIVERSIDADE FEDERAL DE PERNAMBUCO

DEPARTAMENTO DE FÍSICA

DECODIFICAÇÃO PROBABILÍSTICA DE CÖDIGOS LINEARES

Ricardo Menezes Campello de Souza

Tese apresentada ao Departamento de Física da Universidade Federal de Pernambuco como parte dos pre-requisitos para a obtenção do título de Mestre em Ciências.

Prof. **VALDEMAR C. ROCHA Jr.**

Orientador

AGRADECIMENTOS

Gostaria de expressar meus agradecimentos à CAPES e ao Departamento de Física pelo apoio financeiro concedido durante a elaboração deste trabalho. Ao professor Orlando R.Baiocchi, que tornou possível a realização de meu curso de Mestrado. Ao professor Clylton G. Fernandes pelo auxílio prestado em computação. A senhorita Rosa Maria Alves pela dedicação com que datilografou os originais manuscritos e, em especial, ao professor Valdemar Rocha Jr. por sua constante orientação, incentivo e amizade.

RESUMO

Nos últimos anos tem havido ura crescente interesse na decodificaçao probabilística de códigos lineares, isto £, na utilização de sistemas para deteção e correção de erros que usam decisão suave. O que se pretende, e evitar a degradação em desempenho que resulta quando se empregam detetores de apenas duas regiões de quantização antes da decodificaçao, em comparação com os procedimentos ótimos de deteção.

Neste trabalho e feita uma descrição geral da decodificação probabilística de códigos de bloco lineares. Nos três primeiros capítulos são apresentados os conceitos básicos relativos a este tipo de código. No capítulo 4 introduzimos a noção de decisão suave e analisamos o desempenho de alguns algoritmos de decodificação subõtimos. Um algoritmo ótimo é então apresentado e seu desempenho e obtido [1] através de^ simulação em computador. No capítulo 5, os resultados obtidos por simulação são analisados, em comparação com procedimentos que não empregam decisão suave, e algumas sugestoes para futuras investigações são feitas.

ABSTRACT

In the last few years there has been a growing interest in the probabilistic decoding of linear codes, i.e, in the utilization of error detecting and correcting sys terns that use soft decision. The intention is to avoid the degra dation in performance that results when hard decision quantisa - tion precedes decoding, in comparison with optimum detection procedures.

This work presents a general description of probabilistic decoding for linear block codes. In the first theree chapters the basic concepts of such codes are presented . In chapter 4 we introduce the idea of soft decision and analyse the performance of some suboptimum decoding algorithms. An optimum algorithm is then discussed in detail and its performance is obtained by computer simulation. In chapter 5 the computer simulated results are analysed, compared with procedures that do not use soft decision, and suggestions for : future research are made.

I N D I C E

PÁGINA

PAGINA

ÍNDICE DE FIGURAS

FIGURAS

LISTA DE SÍMBOLOS E ABREVIAÇÕES

a - "Byte" de confiabilidade

A - Amplitude de um pulso binário

AN - Sequencia de entrada em um canal discreto sem memoria

ARQ – Automatic repeat request

BCH – Bose - Chaudhuri – Hocquenghem

BSC – Binary symmetric channel

c - Numero de dígitos de paridade de ura código de bloco

C - Capacidade, de canal

C(n,k,d) – Código de bloco de parâmetros n,k e d

C(x) – Polinómio resto

t 1 (n-t)I

CCITT - Comitê Consultatif International Télégraphique et Téléphonique

d - Distância mínima de um código de bloco

d_s - Distância suave

d(u,v) - Distância de Hamming entre as n-uplas u e v

DMC – Discrète memoryless channel

Ce] - Vetor erro

e(x) – Polinómio erro

erf(x) – Função erro

erfc(x) - Função erro .complementar

E – Eficiência

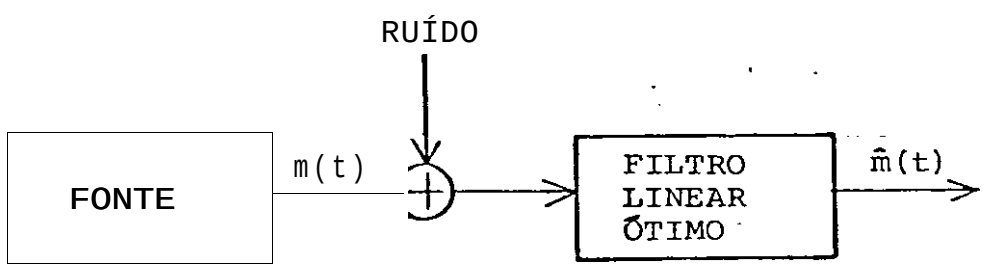
E(R)	- Função expoente de erro
g(x)	- Polinómio gerador de um código cíclico
CG] ''	- Matriz geradora de um código linear
GF(q)	- Campo de Galois de q elementos
[H]	- Matriz de teste de paridade de um cÕdgio linear
1^	– Matriz identidade de ordem K
j	- Amplitude da zona nula de deteção
k	- Numero de dígitos de informação em um código de bloco
Cm)	– Bloco de mensagem
m(x]	- Polinómio mensagem
n	- Comprimento de um código de bloco
N	- Valor normalizado da amplitude da zona nula
p_{0}	– Probabilidade de que um dígito binário transmitido seja recebido erradamente
P_{av}	- Potência disponível
P_{e}	- Probabilidade de erro no canal
p_{c}	- Probabilidade de erro na saída do decodificador
PCM	- Pulse Code Modulation
q_{0}	– Probabilidade de que um dígito binário transmitidi seja recebido corretamente:.
Q	- Número de níveis de quantização
rem	- Resto de uma divisão
(r]	- Palavra recebida
r(x)	- Polinómio recebido
R	– Taxa de informação
R^	- Região nula de deteção
[s)	– Síndrome

SNR	- Relação sinal/ruído
a	— Desvio padrão
t	- Capacidade de correção de um cõdigo de bloco
t	— Capacidade de correção suave de um código de bloco
TDM	— Time division multiplexing
Cu)	- Palavra código
u(x)	— Polinómio código
V_n	- Espaço vetorial das n-uplas
	- Nulo
	- Maior inteiro < X
-CX)	- Matriz X
CX)^T	- Transposta de [X]
to(v)	— Peso da n-upla v
->£p—>	— OU-exclusivo de duas entradas

CAPITULO I

ALGUNS ASPECTOS DA TEORIA MATEMÁTICA DA COMUNICAÇÃO

A teoria da Comunicação deu seus primeiros pas sos em 1924 quando Nyquist ^ mostrou que a taxa de transmissão de pulsos em um canal de banda limitada é proporcional â largu ra de faixa do canal. A partir dal, com exceção de alguns pou- cos trabalhos, as contribuições mais importantes surgiram cora (21 Norbert Wiener e Claude Shannon nos anos 40. Wiener em 1942, conseguiu resolver o problema da filtragem linear ótima, isto¹ é, determinou o filtro linear cuja salda rã(t) é a melhor esti- mativa para m(t), no sentido de minimizar o erro médio quadrá- tico. O diagrama seguinte mostra a configuração analisada por Wiener,.



Shannon [1], seis anos mais tarde, mostrou que sob certas condições, as limitações em desempenho impostas pelo ruído podi-am ser superadas. Desde então, a teoria da comunica- ção teve um grande desenvolvimento, chegando ao estado avançado em que se encontra hoje-Neste, capitulo faremos uma descrição ' geral dos problemas que afetam o desempenho dos sistemas de co

municaçao e introduziremos o conceito de codificação de canal, bem como os principais tipos de códigos e algumas de suas apli caçoes.

1.1 SISTEMAS DE COMUNICAÇÃO DIGITAIS

A teoria da comunicação trata dos sistemas destinados â transmissão de informação. O diagrama de blocos da figura 1.1 representa, de uma maneira geral, um sistema desse [1] tipo.

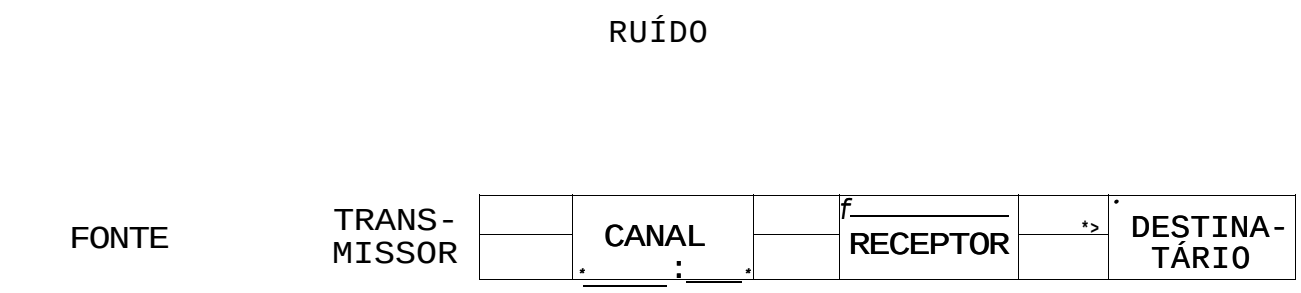


FIG.1.1 - DIAGRAMA DE BLOCOS DE UM SISTEMA DE COMUNICAÇÃO

A fonte de informação pode ser, por exemplo, a voz humana, ou um computador que gera -dados binários, ou ainda um míssil era um sistema de deteção por radar. O bloco transmissor representa, na verdade, o conjunto de dispositivos e/ou circuitos destinados a produção de um sinal ^elétrico correspondente a mensagem da fonte de informação, adequado para transmissão sobre o canal. Em ura sistema telefônico , esta operação consistiria basicamente em se ter sinais elétricos proporcionais ãs ondas de

pressão produzidas pela voz humana. Em um sistema de multiple xagem por divisão de tempo CTDM] que utiliza modulação por código de pulso CPCM]/ cada sinal elétrico associado a uma dada mensagem deve ser sucessivamente amostrado, comprimido, quantizado e codificado; em seguida o conjunto de mensagens é grupado adequadamente de modo a construir o sinal PCM/TDM (4)

O canal ê o meio físico usado para se enviar o sinal do transmissor ao receptor. Ele pode ser, por exemplo., um par de fios, um cabo coaxial, ou mesmo o espaço ' livre, como i o caso de um enlace de radio frequência. Durante a transmissão através do canal, o sinal sofre diversas perturbações(desvanecimento seletivo, ruído, distorção, etc} de modo que a forma de onda que alcança o receptor não é a mesma enviada pelo transmissor. Sendo assim, o bloco receptor representa o conjunto de dispositivos e/ou circuitos destinados a processar o sinal recebido de modo a entregar ao destinatário uma réplica da mensagem gerada pela fonte de informação.

Nos últimos anos tem havido um rápido [1] crescimento na utilização de sistemas de comunicação digitais, isto é, sistemas onde a mensagem já está em forma digital ou ê convertida para este formato, como no caso dos sistemas PCM/TDM. Um diagrama de blocos típico, representativo de um sistema de comunicação digital está mostrado na figura 1.2.

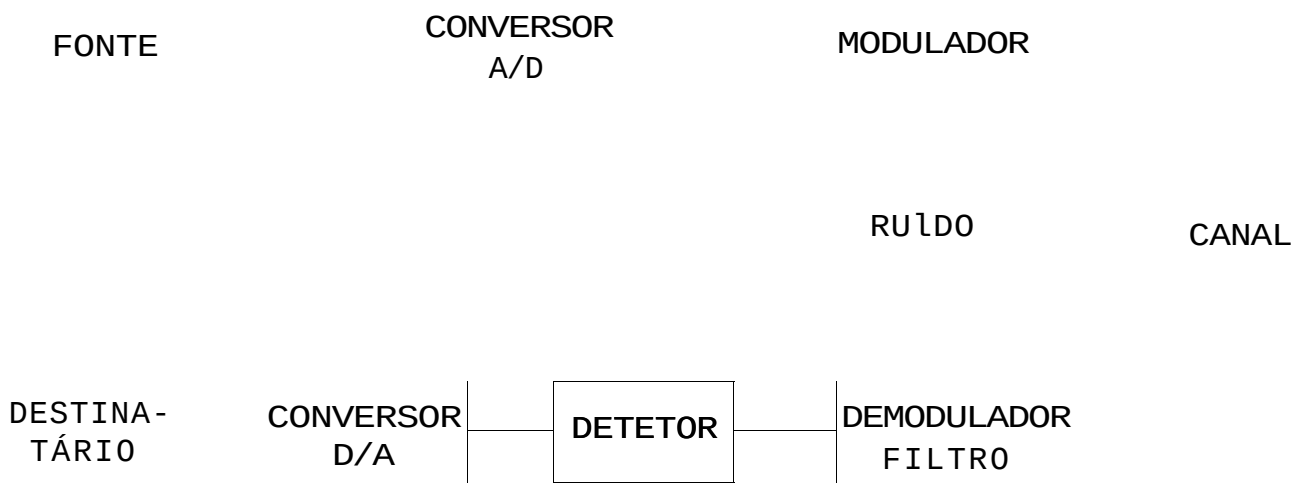


FIG.1.2—DIAGRAMA DE BLOCOS DE UM SISTEMA DE COMUNICAÇÃO DIGI - TAL.

Para compreendermos melhor os problemas pertinentes a um sistema desse tipo, passemos a analisar detidamente as formas de onda presentes em alguns estágios do diagrama de blocos da figura 1.2- Consideremos que a salda do conversor analõgico/digital, isto ê, a forma digital da mensagem f(t) é a que está mostrada na figura 1.3a. Os bits de informação ocorrem a cada intervalo de R segundos de modo que R representa a taxa de transmissão, em bits por segundo. Durante a filtragem do sinal, seja por necessidade ou pela própria resposta em frequência do canal , a energia de cada pulso tende a se espalhar, de modo[1] que pulsos adjacentes tendem a se superpor. Isto provoca o que

é denominado interferência entre símbolos (FIG.1.3b), a qual deve ser

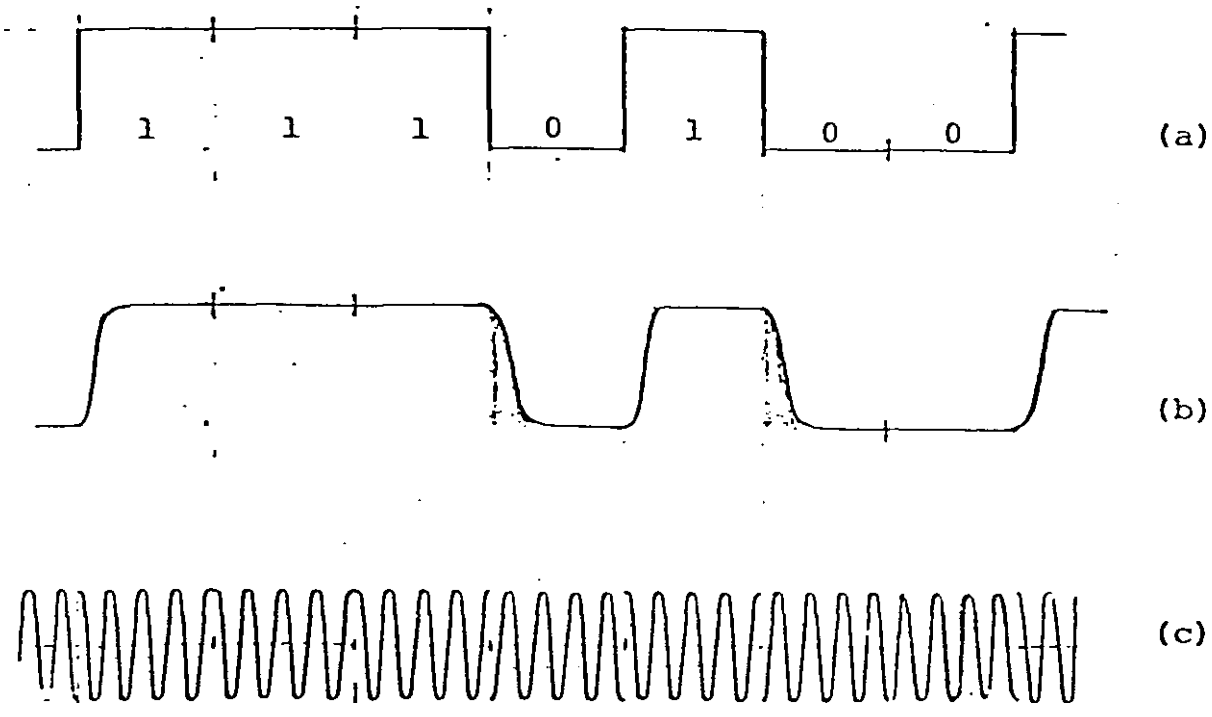


FIG-1-3-FORMAS DE ONDA PRESENTES NO DIAGRAMA DA FIG.1.2(TRANSMISSOR) .

mantida a um nível mínimo, de modo a evitar interpretações errôneas dos bits na recepção, Na figura 1.3c está representada a [1] forma de onda que teria o sinal se o mesmo sofresse uma modulação de fase, antes de ser transmitido^^. Dependendo da natureza do meio transmissor esta operação (modulação) pode se tornar fundamental para o desempenho do sistema, como é o caso de um enlace de HF, onde os sinais sao enviados através de antenas para o espaço livre.

Durante sua passagem pelo canal o sinal[1] sofre perturbações de diversos tipos. O termo ruído representa, em um sentido amplo, qualquer sinal presente no canal que nao seja o desejado. Na maioria dos casos sua ocorrência ê um fenômeno do tipo aleatório, como mostra a figura 1.4a. Se o mesmo soma-se a mensagem, então a salda do bloco demodulador[1] é como a da figura 1.4b e o ruído é dito aditivo. Uma maneira de recuperar a informação na sua forma digital original, seria amostrar o sinal recebido como se vê na figura 1.4b. O sinal recuperado está na figura 1.4c.

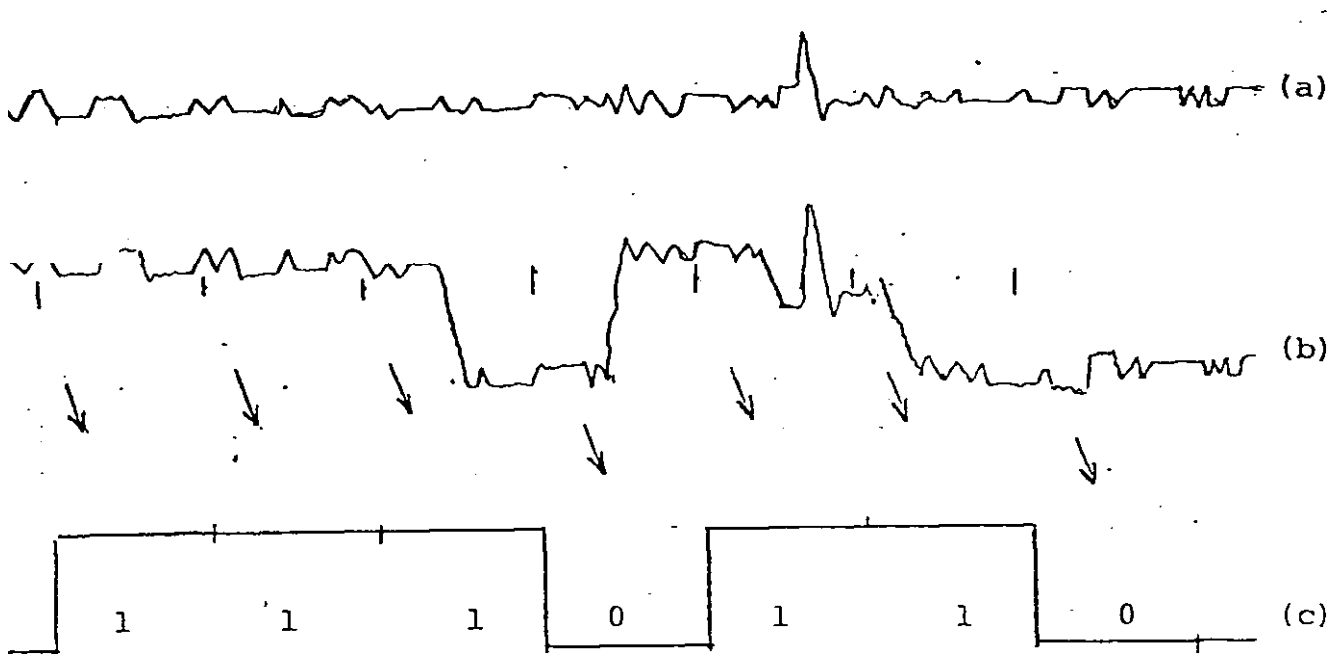


FIG-1.4-F0RMAS DE ONDA PRESENTES NO DIAGRAMA DA FIG.1.2(RECEPTOR).

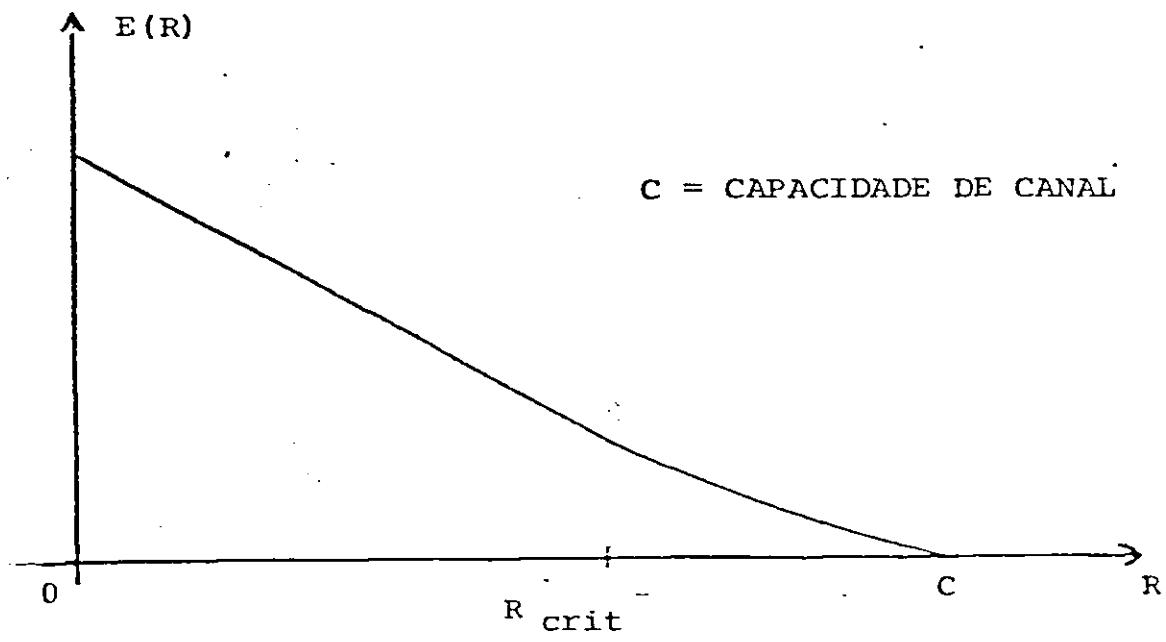
Para que a decisão sobre a ocorrência de um pulso seja confiável é preciso que a relação sinal/ruído no detetor permaneça acima de um certo nível. Por outro lado, devido a limitação existente na relação sinal/ruído (a potência do transmissor não pode ser arbitrariamente grande) .é uma tarefa bastante difícil eliminar completamente a ocorrência de erros no sistema, de modo que estes sempre tenderão a ocorrer, em maior ou menor quantidade- Na figura, observe que o sexto dlgito detetado nlo está correto.

O objetivo de qualquer sistema de comunicação ê transmitir "informação de um ponto a outro, de maneira eficiente, simples e barata. O compromisso inerente a esta afirmação ê obvio de modo que é preciso definir-se um critério para qxie se possa afirmar--que um dado-sistema é ótimo. Considerando apenas o aspecto da eficiência, a questão que surge naturalmente é se, para um dado canal de comunicação, ê possível transmitir informação com uma ocorrência de erros tao baixa quanto se queira.-Esta é uma questão fundamental, uma vez que se a resposta for negativa, não haverá sentido em se tentar construir sistemas mais complexos. Apresentada de forma mais precisa, o que se quer saber exatamente é: Sendo fixadas a potência disponível (P , em watts)e a taxa de transmissão(R, em
av
bits/seg), é possível, para um dado canal, reduzir a taxa de erros a um valor arbitrariamente pequeno? A resposta a esta pergunta foi dada por Claude Shannon, em 1948, em um trabalho que representa um marco no estudo das Comunicações^"^ . Shannon desenvolveu uma teoria matemática da comunicação, depois chamada da Teoria da Informação, destinada "a lidar com os aspectos

mais fundamentais dos sistemas de comunicação. As caracterlsticas principais desta teoria são (1) a abordagem estatística da transmissão da informação (os fenômenos que afetam o desempe - nho de um sistema de comunicação são essencialmente desta natureza) e **(2)** um grande destaque ao problema da existência de técnicas de codificação capazes de reduzir a probabilidade de[1] erros na recepção. Entre outros resultados, Shannon mostrou que, para mensagens de duração T segundos, enviadas através de um canal binário simétrico gaussiano,-a probabiliôade õe erro está limitada superiormente através de

$$Pe < e - \wedge \wedge J \qquad (1.1)$$

onde E(R), uma função chamada expoente de erro, tem a forma geral mostrada na figura 1.5 e C representa a mais alta taxa de transmissão para a .qual E(R) é não negativo.



FJG. 1-5 - FUNÇÃO EXPOENTE DE ERRO

Da expressão vemos <jue P pode ser feita tão pequena ' quanto se queira, para um dado K tal que E(R)>Q, aumentando a duração T do sinal.

Neste trabalho não trataremos da Teoria ' da Informação e o leitor particularmente interessado no assunto deve dirigir-se às referências (3], (6), (7} e (8). O que queremos enfatizar todavia, é a existência de resultados como o da expressão (1.1), baseados em uma teoria matemática bem estabelecida, e a possibilidade de se vislumbrar algoritmos , passíveis de implementação prática, para obtenção de tais resultados. Os códigos corretores de erros representam uma tentativa extremamente importante neste sentido e a abordagem [1] proposta neste trabalho representa, em muitos casos, uma melhora em relação aos resultados obtidos até agora.

1.2 CANAIS DISCRETOS SEM MEMORIA

Para que se possa antecipar o desempenho[1] de um sistema de comunicação e encontrar técnicas que permitam aumentar'sua eficiência é de fundamental importância que se tenha informação precisa sobre o canal de transmissão. Sendo assim, é necessário'se estabelecer um modelo matemático [1] que simule as características do canal, o que implica na especificaçao dos seguintes elementos:

(1) - O conjunto das possíveis entradas do canal.

(2) - O conjunto das possíveis saídas do canal.

(3) - As probabilidades de transição relacionando os conjuntos acima.

Modelos das mais diversas complexidades existem para diferentes tipos de canais [9], porem a realidade física nunca é tão simples de modo que possa ser exatamente representada por um modelo matematicamente tratável. Entre os modelos de canais largamente utilizados no estudo das comunicações está o chamado Canal Discreto sem Memória (DMC), o qual será considerado neste trabalho. Para este tipo de canal, as possíveis entradas e saídas pertencem a um alfabeto finito de símbolos e cada par de entrada e saída está estatísticamente relacionado através de uma probabilidade de transição. Consideremos, por exemplo, um canal discreto sem memória cujo alfabeto de entrada A consista dos L inteiros 0,1....L-l e cujo alfabeto de saída B consista dos M inteiros 0,1,....M-l. O canal é então caracterizado por um conjunto de probabilidades de transição {P(m|£.)}, 0 < £ <1>~1 e 0 < m < M-l. Por definição, P(m|£) significa a probabilidade de se ter, na salda do canal, o inteiro m , dado que o inteiro £ é a entrada do canal. Um canal discreto sem memória é representado esquematicamente como mostra a figura 1.6

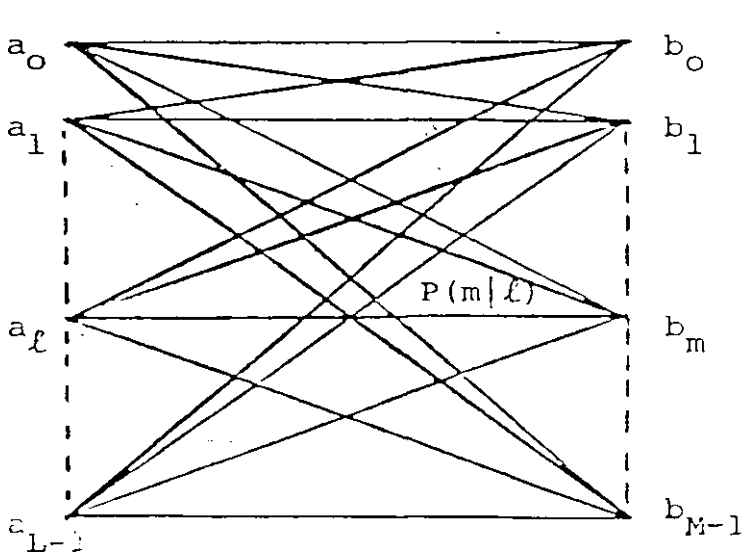


FIG.1.6- CANAL DISCRETO SEM MEMÓRIA.

A denominação sem memória significa que as saídas no instante t_o dependem apenas das entradas naquele instante, sendo independentes de entradas e saídas anteriores. Dito de outra forma, se $7^{\wedge}_{N}=(a_0, a_1, .$ [illegible] representam, respectivamente, sequências-de entrada e saída do canal, então a probabilidade de se ter $B^{\wedge}$ dado $A^{\wedge}$ é dada por

$$P(B \text{ NÍV } " f f \; P(b J a n J \quad U * 2)$$

iU0

Um dos modelos de canais largamente usado na avaliação do desempenho dos sistemas de comunicação e que satisfaz as condições acima, é aquele em que se tem

$$A = B = \{0,1\} \qquad - \qquad (1.3)$$

Esquematicamente, este canal, denominado canal binário simétrico (BSC), está representado na figura 1.7.

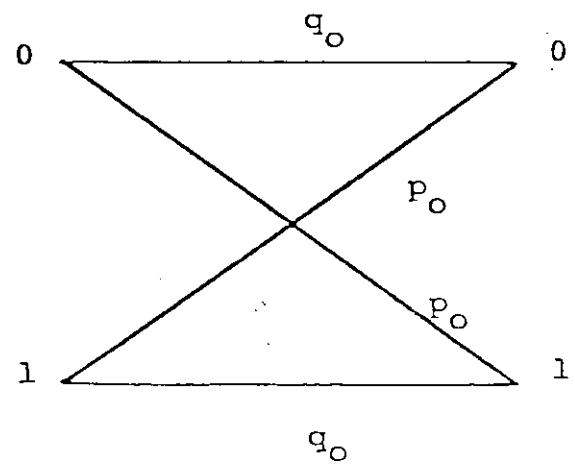


FIG.1.7–CANAL BINÁRIO SIMÉTRICO.

Os números q_Q e p_Q sao aa probabilidades de recepção respectivãmente correta e errônea, em relação ao símbolo transmitido . A probabilidade de se tomar uma decisão errada na recepção depende das propriedades estatísticas do ruídòi que ocorre na transmissão. Em um canal binário simétrico, se as sequencias a_N e B_N diferem em d posições , a probabilidade de erro na recepção será dada por

$$P_e = \sum_{n=0}^{N-l} \binom{N}{n} p^n q^{N-n} \qquad (1.3)$$

$$P_e = 1 - \sum_{n=0}^{N-d} \binom{N}{n} p^n q^{N-n}, \qquad (1.4)$$

onde

$$P(b_i|a_i) = \begin{cases} q, & \text{se } b_i = a_i \\ p, & \text{se } b_i \neq a_i \end{cases} \qquad (1.5)$$

Como em geral $p < q$, então P_e cresce monotonicamente com d , de modo que escolher A_i no sentido de maximizar $P(B|A_i)$ é equivalente a escolher aquela sequência que difira de B_N no menor número de posições. Se A_i é uma palavra de um dado código, este processo de decodificaçao ê chamado decodificação por semelhança máxima. Esta e outras técnicas de decodificação serão discutidas no Capitulo 3.

1.3 CÕDIGOS CORRETORES DE ERROS .

Desde o surgimento dos trabalhos de Shannon, um grande esforço tem sido feito nas pesquisas dedicadas ao problema de projetar esquemas eficientes que permitam a trans-

missão de informação, de maneira confiável, através de canais de comunicação reais, i.e canais sujeitos aos problemas de ruído, distorção, interferência entre símbolos, etc. Neste sentido, a codificação de canal representa, até agora, um dos esforços mais bem sucedidos. Por codificação de canal, entende-se a adição controlada de redundância a uma mensagem, no sentido de protegê-la de eventuais distúrbios provenientes do canal. A redundância adicionada permite, em muitos casos, a proteção e mesmo a correção dos erros que ocorreram na mensagem. Códigos que se destinam a realizar tais objetivos são chamados códigos corretores de erros. De um ponto de vista prático, a principal limitação destes tipos de códigos tem sido a complexidade dos circuitos decodificadores, o que tem [1] orientado as pesquisas no assunto para a obtenção de esquemas de fácil implementação. Entretanto alguns fatores tem contribuído de forma significativa para a utilização cada vêz maior de códigos corretores de erros em sistemas de comunicação. Entre eles poderíamos citar:

(1) - O grande desenvolvimento na tecnologia de circuitos integrados digitais, o que tornou possível a implementação de esquemas codificadores/decodificadores que seriam proibitivos há alguns anos atrás.

(2) - O rápido crescimento de sistemas de comunicação cuja taxa de erros tolerável é muito baixa (computadores-e satélites, p.ex.).

(3) - 0 desenvolvimento da própria teoria de códigos cora a descoberta de técnicas de codificação e~decodificação eficientes como. por exemplo,_a decodificação de limiar^.í^ ,o algorít

mo para decodificar códigos BCH de Berlekamp [12], a decodifica
ção sequencial de Wozencraft, o procedimento de Viterbi pa
ra códigos convolucionais^^, etc.

(4) - A comprovação, através de, simulação em computador e de testes em canais reais, de que sistemas que utilizam códigos[1] apresentam uma sensível melhoria em desempenho, com uma menor' probabilidade de erro para uma dada relação sinal/ruído. Valores típicos da redução obtida sobre P_e são da ordem de 10 ^.

A idéia da utilização de redundância no combate aos efeitos produzidos pelo ruído pode ser entendida de forma simples através do exemplo dado a seguir. Consideremos o seguinte texto recebido, em língua portuguesa, correspondente' a uma mensagem enviada por telegrama:

"VOCE FOI ACEETO PARA O PROGLAMA DE
DOUTORAMELLO DA NOSSO UNEBIRSIDADE
VG QUE SE IMICIA EM 25 DE SETELDRO
PROXIRO."

Percebe-se que os erros existentes na mensagem recebida podem' ser facilmente detetados e corrigidos, tornando imediata a com preensão do texto. Isto se deve â alta redundância presente na língua portuguesa, no sentido de que muitas combinações de le-tras simplesmente não ocorrem, tornando possível sua identificação e consequente correção. Surge, porém, uma dúvida em relação ao número 25. Estaria o mesmo correto? Ou a data originalmente transmitida foi 15? Ou 24? Claro que não poderia ser 35, entretanto a dúvida não pode ser prontamente esclarecida, uma

vez que combinações numéricas do tipo acima usam pouca ou nenhuma redundância e assim qualquer número inteiro $1 < M < 30$ poderia/ter ocorrido. Se, em vez de apenas 25 tivéssemos, por exemplo, SEGUNDA-FEIRA 25 DE SETEMBRO, então a redundância [1] acrescentada permitiria a deteçao de erros e talvez a correção dos mesmos.

Em um sistema de comunicação digital, as sequências binárias de informação nao possuem, por si próprias, nenhuma redundância, de modo que é impossível detetar a presença de erros que possam ter ocorrido durante a transmissão. Para que isto seja conseguido, é necessário acrescentar-se à mensagem bits extras que, embora nao conduzindo nenhuma [1] informação nova, permitem a deteção e/ou localização dos erros. Para esclarecer melhor as afirmações acima considere, por exemplo, o seguinte conjunto de mensagens binárias:

0 0 0 1 0 0
0 0 1 1 0 1
0 1 0 1 1 0
0 1 1 1 1 1

Vê—se que o mesmo nao contém redundância desde que estão presentes todas as palavras formadas por três caracteres binários. Se definirmos a eficiência de uma mensagem como sendo a relação entre a informação contida na mesma e a máxima informação possível de ser transmitida e consideramos que as 8 mensagens sao igualmente prováveis, então teremos:

$$E = \frac{\log 8}{3 \log_2 2} = 100\% \qquad (1\text{-}6)$$

e a redundância

$$1 - E = 0\% \qquad (1.7)$$

O resultado (1.7) significa que não há nenhuma possibilidade[1] de deteçao/correção de erros para as 8 mensagens. De fato, a ocorrência de qualquer configuração de erros sobre alguma palavra, converte-a em outra palavra igualmente válida. Considere agora que um bit extra é adicionado a cada mensagem de acordo com a seguinte regra: Se o número de 1's da palavra é par, então o bit extra é 0 (zero) e em caso contrário é 1; ou seja, o quarto bit i calculado através da soma módulo 2 dos caracteres da palavra. Procedendo assim, formaríamos o seguinte conjunto de mensagens:

0	0	0	0	1	0	**0**	1
0	0	1	1	1	0	1	0
0	1	0	1	1	1	**0**	0
0	1	1	0	1	1	1	1

Admitamos que a palavra 0 0 11, tendo sido transmitida, sofreu uma alteração na segunda posição e foi recebida como * 0 1 1 1. Recalculando o bit redundante vê-se que o mesmo deveria ser 0 e nao 1, de modo que assim detetamos a presença ' de um erro. Observe que sempre que ocorrer um número par de erros, estes não poderão ser detetados. Por outro lado, a não verificação do bit de paridade acrescentado implica apenas na ocorrência de um número impar de erros. 0 preço pago por esta capacidade de deteção está na diminuição da eficiência, pois agora

$$E = \frac{\log_2 8}{4 \log_2 2} = 75\% \qquad \text{Cl-10)}$$

$$1 - E - 25\% \qquad \text{(1-11)}$$

Há então um compromisso entre eficiência de transmissão e capacidade de controle sobre os erros, cuja solução ôtima é função das características particulares de cada problema. O código descrito acima e um -código de um bit de paridade (redundância) e pertence â classe dos códigos de bloco lineares, descritos no capitulo 3.

O diagrama de blocos da figura 1.8 [1] descreve um sistema de comunicação digital que faz uso da codificação de canal.

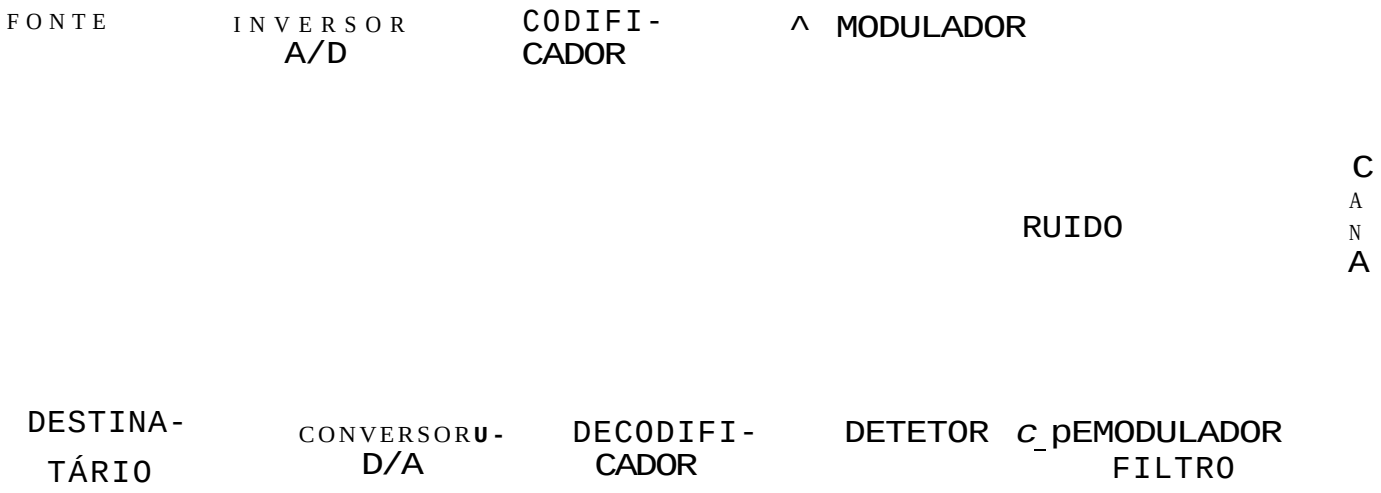
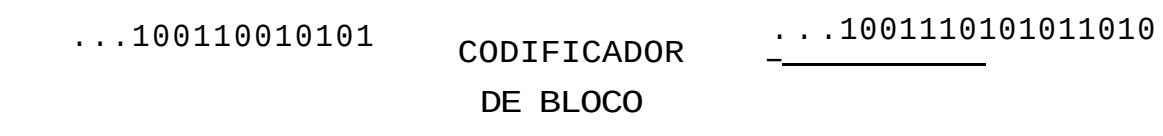


FIG.l-S - SISTEMA DE COMUNICAÇÃO DIGITAL COM CODIFICAÇÃO DE CANAL,

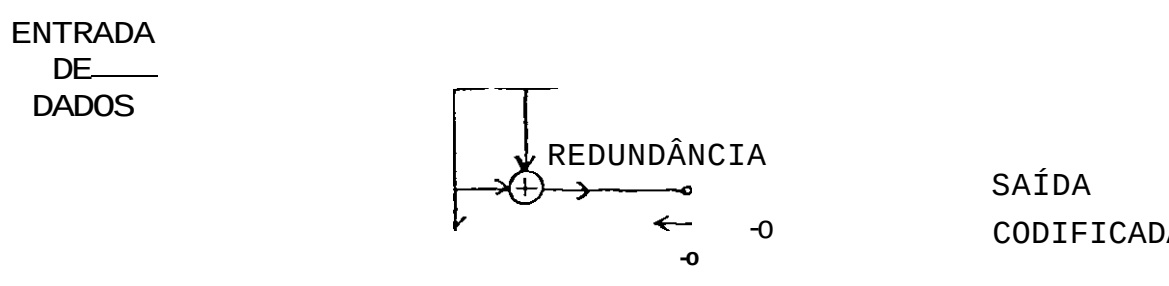
A escolha do tipo de código a ser usado é função de muitos fatores e nem sempre é uma decisão fácil de ser tomada. De uma maneira geral, entretanto, códigos de aplicação prática devem ter uma boa capacidade de deteçao e correção de erros, ser eficientes (i.e. usar pouca redundância) e de fácil implementação. A obtenção destas características tem sido a meta dos pesquisadores nesta área, cujo trabalho teve início há quase três décadas. Em 1950 (14), Richard Hamming, em um artigo pioneiro da teoria da codificação, encontrou um código capaz de corrigir um erro ou detetar dois erros por palavra. Durante esta década outros códigos foram construídos, porém quase sempre para propósitos específicos. Uma classe importante de códigos capazes de corrigir mais de um erro por palavra foi descoberta em 1959/60 de maneira independente, por Bose/Chaudhuri nos Estados Unidos da América do Norte e Hocquenghem, na França. O surgimento de outras classes de códigos capazes de corrigir t erros por palavra seguiu-se imediatamente, o que representou um grande impulso na abordagem algébrica da teoria da codificação. Nesse aspecto os trabalhos de Reed e Solomon (1960), Bose e Chaudhuri (1960), Hocquenghem (1959), Gorenstein e Zierler (1961), Peterson (1961) e Berlekamp (1963), desempenharam um papel extremamente importante. Desde então a teoria da codificação de canal desenvolveu-se bastante sendo atualmente responsável por uma vasta área de pesquisa. A literatura no assunto é bastante ampla e artigos atuais sobre códigos podem ser encontrados nas referencias citadas no presente trabalho.

1.4 TXPOS DE CÓDIGOS

Dependendo da maneira como se adiciona redundância a uma mensagem, dois tipos básicos de códigos corretores de erros podem resultar. Se o codificador processa a informação em blocos, isto é, secciona a sequência de dígitos de informação em palavras de um dado comprimento e opera de modo independente com estas palavras, o código resultante é chamado código de bloco. Neste caso, a redundância acrescentada a cada bloco serve para corrigir e/ou detetar erros apenas naquele bloco. A operação de um codificador de bloco está mostrada na Figura 1.9.



(a)

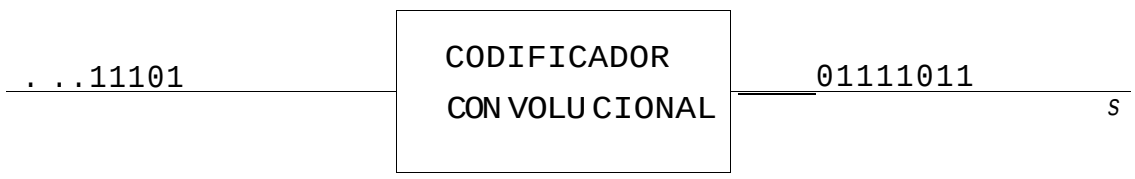


(b)/

FlG.l.9-(a) Procedimento de um codificador de bloco

-(b) Versão simplificada de um circuito codificador.

A outra classe, de códigos, denominada códigos[1] de arvore, é aquela onde a redundância adicionada a cada bloco é função -de mais de um bloco de informação, de modo que estes' não são tratados de forma independente. A subclasse mais importante destes códigos ê a dos "códigos convolucionais, que são mais simples e de mais fácil implementação que outros tipos de códigos de arvore. A operação de um codificador convolucional' está mostrada na figura 1.10



Ca)

(b)

FIG.1-10- (a) Procedimento de um codificador convolucional.
- (b) Versão simplificada de um circuito codificador.

Destes dois tipos de códigos, os códigos de

bloco tem uma teoria mais bem desenvolvida e a razão para isto ê a existência de estruturas matemáticas bem compreendidas associadas a eles. Dessa forma, os mesmos tem sido responsáveis por um maior volume de literatura que os códigos de arvore. Entretanto, ambos tem capacidade de correção e deteçao de erros semelhantes e apresentam certas limitações básicas, de modo que a decisão em favor de um deles é função de fatores como o formato dos dados, o retardo permitido na decodificação, o tipo de canal, a complexidade requerida pára um dado desempenho, etc.

Neste trabalho lidaremos apenas com códigos de bloco, de modo que não consideraremos os códigos de arvore além das definições acima. O leitor interessado neste tipo de códigos deve dirigir-se às referências (13) e (17).

1.5 APLICAÇÕES

Técnicas de codificação de canal, usando códigos convolucionais ou de bloco, vem sendo aplicadas com sucesso a sistemas de comunicação já há vários anos. Em situações onde a probabilidade de erro tolerável pelo sistema é bastante baixa, a transmissão de informação de forma confiável muitas vezes só ê economicamente viável quando se utilizam códigos corretores de erros. A partir de 1970, experiências com canais de HF, canais telefônicos e enlaces de microondas, vieram comprovar a viabilidade da utilização dos códigos corretores de erros em muitas situações de interesse prático. Nesta seção

apresentaremos algumas de suas principais aplicações.

1.5.1 -•TRANSMISSÃO DE DADOS

Segundo as recomendações do CCITT, a taxa de erros em transmissão de dados na rede pública deve ser inferior a 10 ~*, isto ê, em média um bit errado em 10^ transmitidos. Em sistemas que utilizam modems de alta velocidade, com taxas de transmissão superiores a 9600 bits/seg,técnicas de deteção e retransmissão (ARQ) dos dígitos errados tornam-se impraticáveis, de modo que as taxas de erros admissíveis só podem ser alcançadas, sem que o custo e a complexidade do sistema aumentem em demasiado, através do uso de cõdigos corretores de erros. Códigos para correção de erros aleatórios e erros em blocos ("bursts") ..tem -sido usados em sistemas de comunicação por telegrafia, telex e computadores. Exempios típicos de códigos utilizados são ASCII, o código de Hamming e códigos cíclicos.

1.5.2 - ENLACES DE HF

A faixa do espectro correspondente ãs altas frequências de 3 a 30 MHZ é normalmente utilizada para transmissão de sinais de voz e sinais telegráficos via rádio. Estas transmissões sofrem os efeitos de ruído feito pelo homem, de pertubações atmosféricas(variação nas condições de propagação) e de interferência produzida pelos usuários da faixa, normalmente radioamadores.

Devido a esta diversidade de fontes de erros, um sistema de transmissão de dados mesmo bem projetado e trabalhando na melhor frequência disponível apresenta taxas de erro da ordem de 10^{-3} - 10^{-2} por períodos de 5 a 10 minutos. Resultados teoricos e experimentais (9) mostram que a diferença entre estas taxas e a desejada(da ordem de 10 "*) pode ser superada sem • que se perca muito em eficiência, com a utilização de códigos corretores de erros.

1.5.3 COMUNICAÇÃO VIA SATÉLITE

Diversas razões justificam a necessidade da utilização de códigos em sistemas de comunicação via satélite

- Quando uma chamada telefônica atinge o destino errado, ha uma grande diferença se isto ocorre em uma rede urbana ou em um sistema de comunicação via satélite.

- Devido âs limitações de largura de faixa e potência, iê de extrema importância que se transmita informação a uma taxa tão próxima quanto possível da capacidade de canal. Códigos de alta eficiência e complexidade de implementação media permitem uma transmissão "livre de erros e são uma solução econômica para o problema.

- Nas condições ncimais de operação o canal de comunicação por satélite pode ser inodelôâo.por um canal binário simétrico o qual é o mais simples • para controle de erros

Códigos típicos para este tipo de enlace ' são códigos cíclicos, BCH e convolucionais.

CAPÍTULO XI

CÕDrGOS LINEARES

Neste capitulo, serão apresentados os conceitos básicos que definem a estrutura dos códigos linea — res binários de bloco. Estes códigos possuem uma formulação ' matemática bem estabelecida, o que torna sua implementação [1] mais fácil, na. maioria dos casos, em comparação com os cõdi - gos do tipo não linear. Examinaremos alguns tipcs simples de códigos de bloco, bem como sua subclasse mais importante, que são os códigos cíclicos.

2.1 CÓDIGOS DE BLOCO

Um código C(n,k,d) ê um conjunto de 2^k n-uplas binárias, chamadas palavras código, as quais diferem[1] entre sí pelo menos em d posições e formam um subespaço do es paço vetorial-V de todas as n-uplas. O processo de codifica- ção consiste basicamente de duas etapas:

(1) - Os dígitos de informação sãò segmentados em blocos de comprimento k.

(2) - Cada bloco de informação ê transformado em outro bloco de comprimento n(n>k). Os (n-k) dígitos acrescentados ' ao bloco de comprimento k são chamados dígitos de tes te de paridade e representam a redundância que vai per mitir a deteção e/ou correção de erros que venham a ocorrer no sistema de comunicação.

Para os códigos lineares q-ários,sen do q uma potência de um primo, os dígitos de paridade são

calculados a partir da soma modulo q dos dígitos de informação.. Isto é equivalente a dizer *que.* um código (n,k,d) é linear se e somente se o conjunto das 2 palavras código ê um subespaço do espaço vetorial de todas as n-uplas .

A seguir apresentamos um exemplo que esclarecerá melhor os conceitos atê aqui definidos.

EXEMPLO 2.1 -

Considere o código 0(7,3,4), cujas equações de teste de paridade são

$$c_1 = k_1 + k_2$$
$$c_2 = k_2 + k_3$$
$$c_3 = k_1 + k_3$$
$$c_4 = k_1 + k_2$$

Assim, cada bloco de informação de 3 dígitos ê codificado em uma palavra código de 7 dígitos, como mostra a tabela abaixo.

MENSAGEM			PALAVRA - CÕDIGO						
k_1		k_3		k_2	k_3	c_1	c_2	c_3	c_4
0	0	0	. 0	0	0	0	0	0	0
0	0	1	0	0	1	0	1	1	1
0	1	0	0	1	0	1	1	0	1
1	0	0	1	0	0	1	0	1	1
0	1	. 1	0	1	1	1	0	1	0
1	0	1	1	0	1	1	1	0	0
1	1	0	1	1	0	0	1	1	0
1	1	1	1	1	1	0	0	0	1

Desde que K=3, existem 8 mensagens diferentes que são codificadas em oito sextuplas, formando um subespaço de dimensão 3 sobre o espaço vetorial das sextuplas.

2.2 FORMULAÇÃO MATRICIAL

Sabemos da álgebra linear (apêndice A) * que se S^ representa um subespaço do espaço vetorial de todas as n-uplas, é possível encontrar K n-uplas linearmente* independentes em S^, que formam'uma base para este subespaço.

S^ tem dimensão:" K - e possui 2 k n-uplas. Este resultado sugere uma maneira de descrever um código linear C(n,k,d) através de uma matriz (k x n), cujas K linhas linearmente independentes formam uma base para o subespaço formado pelas 2 palavras do código. Esta matriz é chamada matriz geradora do cõdigo e tem a forma

$$CG) = \begin{matrix} v. \\ v. \\ v. \\ I \\ 1 \\ I \\ \mathbf{v}. \end{matrix}$$

Dessa forma, as 2 palavras do código pertencem ao espaço linha de [G3,isto é, se [m) = (m^ , . . -m^.) representa um bloco' de informação, então a palavra código correspondente é dada por

$$(u) = ím] (G) = tm ,m_2, . . .m^) \begin{matrix} \mathbf{v}- \\ j\cdot \\ {}_v\wedge \\ j \\ v. \end{matrix} \quad \ldots \quad £2.2)$$

ou $(u) - m_x$ Q/-jp + m_2 [v 2^{3+} ______ + ^{m} v t_k [v v_k) (2.3)

Vê-se então que as palavras de C sao obtidas por combina ções lineares das linhas de[G)e é dito que as linhas detG^ge- rara um código linear C(n,k,d).

EXEMPLO 2.2 -

Vamos descrever o código definido no exem - pio 1 pela sua matriz geradorafG). De acordo com as equações de teste de paridade, cada palavra do código é da forma

Cu) = $ík_x$ k_2 k_3 k-j+fc^ $^_2+k_3$ $k_1+^_3$ $k_1+k_2+k_3$]

cuja representação matricial é

$$Cu) = (k_1 k_2 k_3) \begin{matrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{matrix}$$

sendo assim, o código do exemplo 1 ê um código C(7,3,4) cu ja matriz geradora é

$$\begin{matrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{matrix}$$

De maneira geral, um cõdigo linear C(n,k,d) pode ser descrito por uma matriz geradora, a qual tem ase guinte forma:

OG) -

$$\left[\begin{array}{cccc|cc} 1 & 0 & 0 & 0 & p_{11} & p_{12} \cdots p_{1,n-k} \\ 0 & 1 & 0 & 0 & p_{21} & p_{22} \cdots p_{2,n-k} \\ 0 & 0 & 1 & 0 & p_{31} & p_{32} \cdots p_{3,n-k} \\ 0 & 0 & 0 & 1 & p_{k1} & p_{k2} \cdots p_{k,n-k} \end{array}\right] \qquad (2.4)$$

ou

$$CG] = [I_k \quad P) \qquad (2.5)$$

onde I_k representa a matriz identidade de ordem K e P i uma matriz do tipo K x (n-k).

Uma segunda descrição matricial para os códigos em bloco lineares e a que faz uso da matriz (H}, chamada matriz de teste de paridade. A matriz (H) e construída de modo que o produto escalar de qualquer combinação linear das linhas de (G) por uma linha de (H) e nulo, isto é, $GH^T = 0$. Assim se (19) - nal ao espaço-linha de (G) .

$$CH) = \begin{bmatrix} h_{11} & h_{12} \cdots h_{1n} \\ h_{21} & h_{22} \cdots h_{2n} \\ \vdots & \\ h_{(n-k)1} & h_{(n-k)2} \cdots h_{(n-k)n} \end{bmatrix} \qquad (2.6)$$

$$Cu) = (u_1, u_2, \ldots, u_n) \qquad (2.7)$$

representam respectivamente a matriz de teste de paridade e um vetor do espaço-ÜTiha de *[G)* então devemos ter

$$Cu)\ (H)^{T} = (0\ \ 0\ \ 0 \ldots 0). \qquad (2.8)$$

Dessa forma, Qu)é uma palavra cõdigo do código linear C(n,k,d) gerado por (G)se e só se (2.8) se verificar.

De maneira semelhante a expressão (2.5) a matriz H C(n-k) x n) pode ser colocada na forma

$$£H)= CP^{T} ;\ I_{n\_k}3 \qquad (2.9)$$

onde P^{T} e l_{n_k} representam respectivamente a transposta da matriz P e a matriz identidade de ordem (n-k).

2.3 CAPACIDADE DE CORREÇÃO

Dois tipos distintos de erros podem ocorrer em sistemas 'de comunicação:

(1) Os símbolos transmitidos podem ser afetados de maneira in dependente. São os chamados erros aleatórios.

(2) Em alguns canais ocorrem pextubações cuja duração é maior que o tempo alocado para cada símbolo, de modo que vários deles podem ser afetados consecutivamente. São os chama - dos erros em bloco("burst") .

Neste trabalho trataremos apenas do primei-

ro tipo de erro. Para estabelecermos a capacidade de correção de erros aleatórios de um código linear de bloco C(n,k,d),precisamos introduzir algumas definições.

*

DEFINIÇÃO 2.1 - Seja v uma n-upla binaria. O peso de v , que denotaremos por w(v], e o número de posições não nulas de v.

DEFINIÇÃO 2.2 - Sejam u e v duas n-uplas binarias. A distância de Hamming entre u e v, que denotaremos por d(u,v) , é o número de posições em que as mesmas diferem.

De acordo com as definições acima, vê- se que

$$d(u,v) = w(u \copyright v) \qquad (2.10)$$

uma vez que a operação © representa adição módulo 2.

k

As 2 palavras de um código de bloco li – near C(n,k,d) formam um grupo, de modo que a soma de duas palavras código quaisquer ê uma palavra código. Este fato, juntamente com a expressão (2.10), nos permite concluir que a me nor distância entre duas palavras, chamada distância mínima ' do código, é dada pela n-upla de menor peso, ^excetuando-se a n-upla toda nula, isto é,

$$d = w\ (v\hat{}) \qquad (2.11)$$

onde v representa a n–upla de menor peso de C. Baseado neste

conceito de distância mínima vamos agora determinar a capacidade de correção/deteção de um dado código. Observamos que a ocorrência de um erro em uma palavra transmitida resultara em uma distância de Hamming igual a 1 entre esta e a palavra recebida. Sendo assim, a ocorrência de uma quantidade $<(d-l)$ de $n \quad k$ erros em uma palavra transmitida resultará em uma das $(2 - 2)$ n-uplas que não são palavras código, o que possibilita a detecção de uma dada configuração de erros. Portanto, um código [1] com distância mínima d e capaz de detetar (d-1) erros. Sua capacidade de correção pode ser entendida com o auxílio da k figura 2.1, onde d_{ij} $(i,j=l,2,...,2$, com i / j) representa a distância de Hamming entre as palavras código i e j .Se d representa a

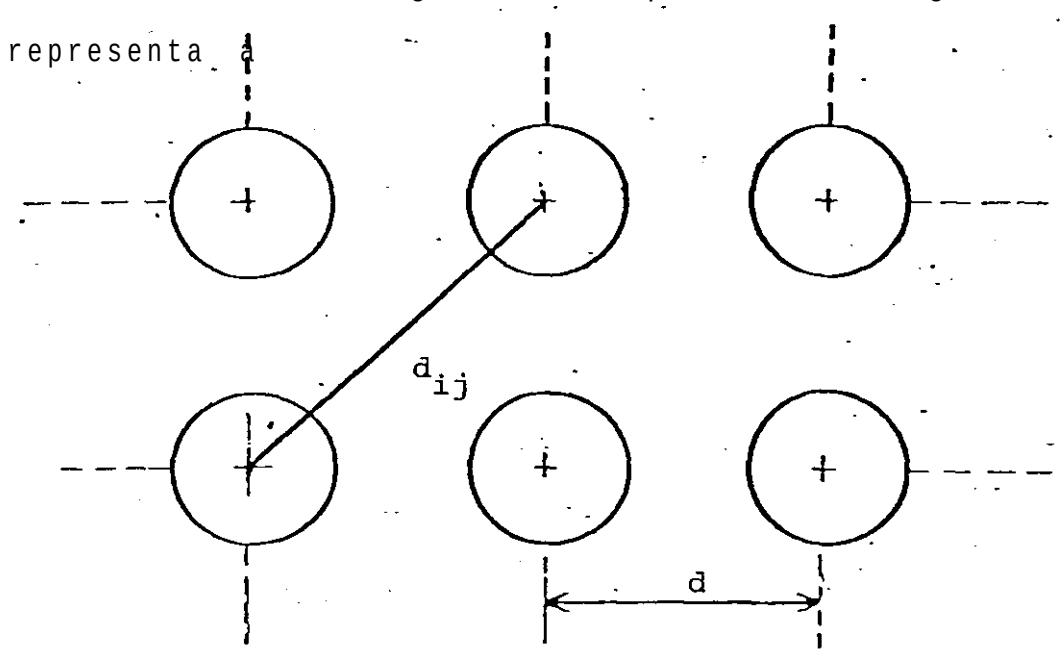


FIG.2.1 - DISTANCIA MÍNIMA DE UM CÕDIGO DE BLOCO LINEAR -

distância mínima, vi-se que a ocorrência de d/2 ou mais erros transformará a palavra transmitida em uma n-upla que es-

tá mais próxima, em termos de distância de Hamming, de outra palavra código. Dessa forma, como o decodificador decide pela palavra que mais se aproxima da n-upla recebida, resultara [1] uma decodificação errada. Para^que a palavra transmitida seja decodificada corretamente devemos ter, então:

$$t < \frac{d}{2} \quad (2.12)$$

onde t representa o número de erros que podem ser corrigi - dos e $\lfloor x \rfloor$ quer dizer o maior inteiro < x.

Assim, o problema de encontrar um código com uma determinada capacidade de correção, consiste básica - mente em achar um código que tenha uma dada distância mínima. Na verdade, sendo, conhecidos n e k, existem limites que esta belecem os valores extremos para d (18). Um dos problemas que ainda permanece sem solução na teoria dos códigos corretores' de erros ê como formar as equações de teste de paridade para garantir um dado d, sendo dados n e k .

2.4 CÓDIGOS DE BLOCO LINEARES SIMPLES

2.4.1 - CÓDIGOS DE REPETIÇÃO

Dentre os exemplos mais simples de cõdi - gos binários encontram—se os chamados códigos de repetição Para este tipo de código tem-se

$k \ll 1$

•c qualquer

$n = k + c = l +$ ₀

de modo que existem apenas duas palavras, que são as sequências de n 0's e n l's. Os dígitos de paridade são todos iguais ao dígito de mensagem. Devido a ocorrência de erros no canal, alguns dígitos são alterados e o decodificador avalia' o numero de 0's e de 1's da palavra recebida, decidindo pelo bit que apareceu mais vezes. Em caso de igualdade (n-par) nenhuma decisão ê tomada. A distância mínima e a eficiência de um código de repetição valem, respectivamente

$$d \quad n$$

$$R = \frac{1}{n}$$

de modo que qualquer configuração de erros que atinja menos que a metade de uma palavra pode ser detetada e corrigida.

2.4.2 - CÕDIGOS DE UM ÜNICO DIGITO DE PARIDADE

Estes códigos são caracterizados por:

1c qualquer

$c = 1$

$n = k + ' c = k + l .$

Devido ao fato de usarem mínima redundância, são códigos de

alta eficiência, a qual é tanto maior quanto fôr o valor de n, pois

$$R = \frac{n-1}{n}$$

Seu único digito de paridade ê gerado pela soma modulo 2 dos n-1 dígitos de informação, de modo que suas palavras são todas de peso par. Sendo assim, um código de um dígito de paridade (SPC) tem distância mínima igual a 2 e ê capaz de detetar qualquer configuração de um número ímpar de erros. Entretanto, apesar desta baixa capacidade de controlar erros, sao largamente usados na prática . Os códigos descritos nesta seção e na anterior representam as soluções extremas para o compromisso capacidade de deteção/correçao versus eficiência, de modo que a maioria dos códigos de bloco lineares situa- se numa posição intermediária em relação aos mesmos.

2.4.3 - CÕDIGOS DE MATRIZ

Estes códigos, em sua forma mais simples, são' obtidos através da extensão, para duas dimensões, dos códigos ' de um dígito de paridade. Dessa forma dígitos de paridade horizontais e verticais são acrescentados a uma matriz retangular ' de dígitos de informação, conforme está ilustrado na figura **2.2**

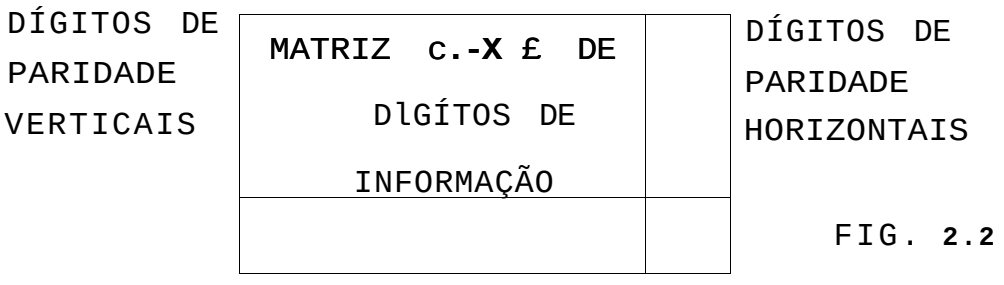


FIG. **2.2**

Devido a dupla verificação de paridade existente, qualquer erro isolado pode ser corrigido, enquanto que todas as configurações de dois erros podem ser detetadas. A eficiência e a distância mínima de um código de matriz valem, respectivamente

$$R = \frac{l * c}{(l+1)(c+1)}$$

$$= 4$$

2.5 CÕDIGOS CÍCLICOS

Grande parte da pesquisa dedicada aos códigos corretores de-erros tem sido orientada no sentido de se obter códigos que estejam associados a alguma estrutura matemática bem definida. A razão para isto e que, devido a esta associação, procedimentos para codificação e decodificação, bem como a estratégia a ser seguida para se conseguir certas características desejáveis, podem ser obtidos com relativa facilidade. Uma subclasse dos códigos lineares binários em bloco que preenche as condições acima, é a dos chamados cÕdigos cíclicos, introduzidos em 1957 por Prange (21). Estes codigos são bastante usados em aplicações praticas e foram responsáveis por grande parte das investigações feitas em códigos de bloco, durante a década de 60. Nesta seção faremos uma descrição sumária dos códigos -cíclicos,-apresentando algumas de suas principais propriedades.

2.5.1 - DESCRIÇÃO GERAL

Um código cíclico em geral é um código de bloco linear C(n,k,d) que possui a propriedade de que qual - quer versão deslocada, de maneira cíclica, de uma palavra código é também uma palavra código. Dessa forma se

Ç> = ᶜᵘ0' ᵘ l ᵘ n - l) ᴱ ᶜ

então

ᵗᵘ 1 = ᶜ ᵘ n - i ' ᵘ n - i + l ᵘ n - l ' ᵘ 0 ' ᵘ l - - - ᵘ n - i - l ˡᴱ ᶜᴵ

onde(u^),por definição representa a n-upla **(U)** deslocada ci - clicamente para a direita, de **i** posições. Para descrever os

_____ _ **Í**(18)

o procedimento que faz uso da correspondência existente entre n-uplas binarias e polinómios racionais com coeficientes em GF(2), o campo de Galois de dois elementos (0.1)(18) . Assim a palavra código

[u) = tu-,u₁«...uₙ_

é representada por

u(x) = **U**Q + u-x + u-x^ + ...ᵘₙ_^ˣⁿ "*~(2.13;

sendo que u(x) ê usualmente chamado polinómio código. A cons- trução de _m código cíclico é baseada na existência de um po-

linômio 9(x) chamado polinómio gerador, para o qual sao vãli-
dos os seguintes teoremas[23]

TEOREMA 2.1 - Em um código cíclicoC{n,k,d) existe um e apenas um polinómio código g(x) de grau (n-k), do tipo

$$g(x) = x^{n-k} + g_{n-k-1}x^{n-k-1} + \ldots g_2 x^2 + g x + 1 \qquad (2.14)$$

de modo que qualquer polinómio código u(x) em C é um múltiplo de g(x) e todo polinómio de grau n-1 ou menor, que ê múltiplo de g(x), é um polinómio código.

TEOREMA 2.2 - O polinómio gerador de um código cíclico(n,k,d) é um fator de $x^n + 1$.

TEOREMA 2.3 - Se g(x) tem grau (n-k) e é um fator de x^n+l, então g(x) gera um código cíclico (n,k,d).

Vejamos um exemplo para ilustrar a construção de um código cíclico.

EXEMPLO 2.3 - O código cíclico (7,4,3) cujo polinómio gerador ê

$$g;(x) = 1 + x + x^3$$

é aquele para o qual as palavras códigos sao da forma

$$u(x) = m(x)\ (1 + x + x^3)$$

onde jnCxJ representa o polinómio mensagem. Assim a mensagem [1] 1100 em forma codificada é

$$u(x) = (1 + x)\ (1 + x + x^3)$$

$$u(x) = 1 + x^2 + x^3 + x^4$$

ou Cu3 = (1 0 1 1 1 0 0)

As 16 palavras deste código estão na tabela abaixo:

MENSAGEM	PALAVRA CÓDIGO
0 0 0 0	0 0 0 0 0 0 0
1 0 0 0	1 1 0 1 0 0 0
0 1 0 0	0 1 1 0 1 0 0
1 1 0 0	1 0 1 1 1 0 0
0 0 1 0	0 0 1 1 0 1 0
1 0 1 0	1 1 1 0 0 1 0
0 1 1 0	0 1 0 1 1 1 0
1 1 1 0	1 0 0 0 1 1 0
0 0 0 1	0 0 0 1 1 0 1
1 0 0 1	1 1 0 0 1 **0** 1
0 1 0 1	0 1 1 1 0 1 1
1 1 0 1	1 0 1 0 **0** **0** 1
0 0 1 1	0 0 1 0 1 1 1
1 **0** 1 1	1 1 1 1 1 1 1
0 1 1 1	0 1 0 0 0 1 1
1 1 1 1	1 0 0 1 **0** 1 1

Estas palavras apresentam os dígitos de" informação. _k-₂'ᵏ3'ᵏ_j* ᵉᵃᵉ paridade (.ᶜi'ᶜ₂'C-] misturados Para colocá-los em forma sistemática, isto é, fazer com que ' cada palavra seja do tipo tk^,k_,,k_./k^, , ,C-,) ê suficien - te[23] - fazermos:

$$v(x) = C(x) + x^{n-k} m^{(x)} \qquad (2.15)$$

onde C(x) e resto da divisão de $x^{n-k} m(x)$ por g(x):

$$C(x) = \text{rem}\frac{x^{n-k} . . m(x)}{g(x)} \qquad (2.16)$$

Nesse caso C(x) representa a seção de dígitos de paridade de cada palavra código. Este resultado permite a formulação de métodos práticos para codificação, os quais utilizam apenas circuitos registradores a deslocamento -com realimentação e so raadores modulo -2[22] . Esta característica de simplicidade dos circuitos codificadores é um dos aspectos extremamente importantes dos códigos cíclicos.

2.5.2 - DETEÇAO E CORREÇAO DE ERROS

A deteção de erros em palavras código.[1] como as do tipo (2.15) pode ser feita de maneira .simples. Des de que as 2^k palavras código - de. C(n,k,d) sao todas múltiplas do polinómio" gerador g(x)uma missão do decodificador -consiste em verificar este fato. De um modo geral"a~palavra"recebida é

$$rCxJ = uCx] + e(x) \qquad (2.17)$$

onde e(x) é o polinómio erro introduzido no canal. Sua divisão por g(x) resulta

$$\frac{r(x)}{g\{x)} = \frac{uÇx)}{g(x)} + \frac{e(x)}{g(x)} = m(x] + \frac{e(x)}{g(x)} \qquad (2.18)$$

Então, se o resultado (2.18) não for exato, a ocorrência de erros durante a transmissão será detetada. Portanto o polinómio gerador.. g(x) deve ser escolhido de tal modo que as configuraçÕes de erros ₑ(x) que se quer detetar nao sejam divisí - veis por ele. Os teoremas enunciados a seguir mostram algumas ^elações entre a capacidade de deteçao de um código cíclico e seu polinómio gerador.

TEOREMA 2,-4 — O número de termos do polinómio -gerador de um código cíclico (n,k,2) ê > 2.

DEFINIÇÃO 2.3 - Um polinómio f(x) pertence ao expoente n se n i o menor inteiro positivo para o qual f(x) divide x^n-l.

TEOREMA 2.5 - O comprimento de um código cíclico (n,k,3) não é maior que o expoente ao qual pertence seu polinómio gerador.

De uma maneira geral, entretanto, não hã uma relação simples entre g.(x) e d ,--a distância mínima do código. Na tabela a seguir apresentamos as principais características de alguns códigos cíclicos de comprimento .i5.

. K .	d	
14	*2*	(0,1)
11	3	(0,1,4)
10	4	(0,1) (0,1,4)*
7	5	(0,1,4) (0,1,2,3,4)
6	6	(0,1) (0,1,4) (0,1,2,3,4)
5	7	(0,1,4) (0,1,2,3,4) (0,1,2)
4	8	(0,1) (0,1,4) (0,1,2,3,4) (0,1,2)
2	10	(0,1) (0,1,4) (0,1,2,3,4) (0,3,4)
1	I⁵ .	(0,1,4) (0,1,2,3,4) (0,3,4) (0,1,2)

TABELA — Alguns códigos cíclicos de comprimento 15.

* O símbolo (0,1) (0,1,4) representa o polinómio:

$$(1 + x)\ (1 + x + x^4) = 1 + x^2 + x^4 + x^5 \qquad (0,2,4,5)\ .$$

Um dos-aspectos mais positivos dos códigos* cíclicos é a ,existência de diversos algoritmos de decodificação eficientes, que podem ser implementados com relativa facilidade. Dentre estes, citamos como mais importantes a decodificaçao de Meggitt (24) (1960), a decodificaçao por lógica majoritária (25) (Rudolph, 1967), e- o método conhecido por "error-trapping .(Rudolph e Mitchell, 1964). Estas técnicas [1] fazem uso essencialmente do conceito de síndrome para localização de erros e a escolha por uma delas é íunção de fatores como o tipo de erro presente no canal, a classe de códigos cí

clicos usada, a capacidade de memória disponível, o retardo na decodificação, etc.

Dentre os códigos cíclicos conhecidos são particularmente importantes os códigos de Bose-Chaudhuri e Hocquenghem. Para qualquer escolha de m e t existe um código BCH de comprimento $2^m - 1$ que é capaz de corrigir t erros ou detetar 2t erros por palavra e que requer um polinómio gerador de grau < mt^^^. O primeiro algoritmo de decodificação para este tipo de código foi devido a Peterson [27]. Alguns anos mais tarde outros procedimentos mais eficientes foram estabelecidos por Chien[28] (1963), Berlekamp[29] (1965) e Massey (1969), de modo que os códigos BCH são de grande aplicação prática e bastante usados nos sistemas de comunicação atuais.

CAPÍTULO I I I

• -PECODIFICAÇÃO DE CÓDIGOS LINEARES

.

A decodificação frequentemente representa um sério obstáculo â utilização prática dos códigos corretores de erros. Isto se deve ao fato de que os algoritmos de decodificação existentes apresentam uma complexidade que cresce exponencialmente com o comprimento dos blocos [22], tornando sua implementação proibitiva. Neste capítulo apresentamos' alguns dos principais métodos existentes para decodificação[1] de códigos lineares, comparando e discutindo a complexidade ' dos mesmos.

3.1 PECODIFICAÇÃO POR SEMELHANÇA MÁXIMA

O método descrito nesta seção raramente é usado na prática devido ãs dificuldades de implementação[1] que apresenta. Sua importância reside no fato de ser largamente usado como um padrão, sempre que se deseja comparar diferentes técnicas de decodificação. Esta técnica, quando se usam palavras código equiprovãveis, ê ótima no sentido de que a probabilidade de erro na saída do decodificador é minimizada

Em um canal binário simétrico, a probabilidade de nao ocorrer erros em uma n-upla binária transmitida é q^{11}. A probabilidade .de que a palavra recebida seja dife-

rente da palavra transmitida em i posições e p_Q q_Q .Desde que q^> p_Q, qualquer palavra com um erro ê mais provável de ser recebida que uma palavra com dois erros e assim por diante. Baseado neste resultado é possível decodificar códigos em bloco lineares como a seguir é descrito. Na recepção o decodificador compara a n-upla recebida Cr) com as 2 palavras' código existentes e escolhe aquela que mais se aproxima de[r3 em termos de distância de Hamming, isto é, decide por aquela palavra que difere de Cr) no menor numero de posições.

Em sistemas operando "on line" esta comparação deve ser feita durante o intervalo de tempo correspondente â duração de n dígitos no canal, o que eventualmente vem a limitar a aplicabilidade deste processo quarido o código utilizado tem um grande numero de palavras. Este método de de codificação por semelhança máxima pode ser aplicado a canais sem memória que não sejam binários.

3.2 O ARRANJO PADRÃO

O processo de decodificação envolve uma decisão sobre qual palavra código foi transmitida. Isto pode ser feito distribuindo as 2^n n-uplas em 2^k conjuntos disjuntos de modo que cada um deles contenha apenas uma palavra código. Desta maneira a decodificação é feita corretamente se a_n-upla recebida Cr) estiver no subconjunto da palavra transmitida. Escrevemos as 2 n-uplas em uma linha e abaixo da n-upla nula colocamos uma n-upla Ce-) que não está na primeira'

linha. A segunda linha ê. formada somando-se os elementos da primeira a Ce_2_, como mostrado abaixo:

C0,0,_____0) CV-] "IV.) '. . . . . CV ,)
2

Ce₂) Ce₂] + CV₂) te₂_ + CV₃). . . . . te₂_ + CVₖ_

As linhas subsequentes são formadas de maneira semelhante , sendo que cada nova linha começa com um elemento não usado anteriormente^" Resulta assim a seguinte tabela, denominada arranjo padrão.

(0,0,...03 ÍV₂) CV-J. . . . . CV 2ᵏ)

Ce2] Ce2] + CV23 Ce23 + CV 3 * Ce 21 + CV k]

Ce₃) Ce₃] + CV₂) te.) + (V-3. . . . . [e₃3 + CV _J

Ce) Ce }+CV-] Ce ,)+[VJ. . . . . Ce ₁}+(v,)
₂n-k ' 2ⁿ⁻ᵏ 2ⁿ~H 2ⁿ⁻ᵏ 2ᵏ

As linhas.obtidas são chamadas "cosets" e o elemento mais à esquerda em cada linha ê o "coset leader". O processo descrito acima é chamado decomposição do código em "cosets". Básicamente, a utilização do arranjo padrão para decodificação envolve dois passos:

1) Determinação do "coset" Ce portanto do"coset leader" associado) ao qual a n-upla recebida pertence.

2) Subtrair da n-upla recebida o "coset leader" encontrado ' acima. .

O resultado obtidp no segundo passo é a estimativa da palavra transmitida. Isto, em geral, não é fácil de implementar, de modo que o conceito de arranjo padrão ê mais útil como uma maneira de compreender a estrutura dos códigos' lineares, do que como um algoritmo de decodificação prática . Entretanto, o arranjo padrão apresenta algumas propriedades ' que nos permitem estabelecer um método de decodificação potencialmente prático, o qual será descrito na seção seguinte. Estas propriedades estão contidas nos dois teoremas que apresentamos a seguir:

TEOREMA 3.1 - Seja C(n,k) um código de bloco binário linear. Então o arranjo ^padrão obtido pela decomposição de C em cosets não apresenta n-uplas repetidas.

PROVA: Consideremos que na j-ésima 1inha existem duas n-uplas idênticas. Então devemos t e r

$$i^{e}j)^{+}C^{v}{}_{e})=r^{e}j\}^{+}[^{v}{}_{m}> \text{ onde } e \wedge m \qquad (3.1)$$

e portanto

$$(v_e) = lv_m)$$

o que é impossível pela própria construção da tabela. Resta ' então mostrar que uma mesma n-upla nao aparece em diferentes[1]

linhas. Considerando que uma n-upla aparece nas linhas i e j (icj), então devemos ter:

$$t_{e_1} + t_{e_j} = C_{e_J} + C_{v_{nv}} \qquad (3.2)$$

então:

$$t_j J = t_i . U \quad (v_e + v_m) \qquad (3.3)$$

desde que v_e e v_m sao vetores códigos, então $(v_e + v_m)$ também é um vetor código, que vamos representar por $\hat{v}$. Dessa forma

$$(e_3) = (e_x) + (v_x) \qquad (3.4)$$

da equação (3.4) concluímos que (e_3) está na i-ésima linha, o que contradiz o fato de que o primeiro elemento de uma linha do arranjo padrão é um elemento não usado anteriormente. Dessa forma a prova está completa.

* Antes de apresentarmos o teorema 2 vamos conceituar o que chamamos de síndrome de uma palavra. Consideremos um código linear em bloco C(n,k,d) cuja matriz de paridade é H. O vetor de (n-k) componentes definido por

$$(S) = (r) (H)^T \qquad (3.5)$$

é denominado a síndrome da palavra r. Da definição de $(\ddot{u})$ vemos que r é uma palavra-do código se e só se sua síndrome

for nula. Na recepção, o decodificador tenta extrair a mensagem enviada a partir de (3.5)- Em geral

$$t r) = Cu) + Ce) \quad (3.6)$$

onde

$$te) = (e_1, e_2, \ldots e_n) \quad (37)$$

representa o vetor erro introduzido pelo ruído no canal, de modo que

$$e. = \begin{cases} 0, \text{ se o ruído não afeta o i-ésimo dígito} \\ 1, \text{ em caso contrário.} \end{cases} \quad (3.8)$$

Ficamos então com

$$CS) = Cu)\ CH)^T + (e)\ (H)^T \quad (3.9^f)$$

$$.CS) = Ce)\ (H)^T \quad (3.10)$$

o que mostra que a síndrome associada a uma palavra código depende apenas da configuração de erros que atingiu a mesma.

TEOREMA 3.2 - No arranjo padrão de um código linear C(n,k,d) as 2 n-uplas de um dado "coset" tem a mesma síndrome e as síndromes de cosets diferentes sao diferentes.

PROVA: Consideremos inicialmente que o m-êsimo e o £-esimo

coset tem síndromes iguais, isto é.

$$te_{m}J\ [K\}^{T} = Ce\hat{}J\ (H)^{T} \qquad (3.11)$$

ou

$$\{te^{m}) + {}^{Ce}Z)\}\ \ in)^{T} = 0 \qquad (3.12)$$

Sendo assim , a n-upla {te^) + é uma palavra código, a qual vamos representar por(u^) Então

$$^{Ce}m^{5} = {}^{Ce}£^{3} + {}^{fu}V\ ' \qquad (3.13)$$

ou seja, o vetor (e^) pertence â í-ésima linha do arranjo padrão, o que nao é possível devido ã forma como o mesmo é construído. Para concluir vamos mostrar que os vetores de um mesmo coset tem a mesma síndrome. Consideremos o j-ésimo "coset", cujo "coset leader" ê fe..}. A síndrome associada a uma n-upla íu^) pertencente a este coset e dada por

$$IS) - íte\hat{}) + Cu_{\pm}n\ tH)^{T} \qquad (3.14)$$

Como tu^)$^{e\ u\ m\ a}$ palavra de C, então (3.14) reduz-se à

$$(S) = te..)\ CH)^{T} \qquad (3.15)$$

que é a síndrome para qualquer membro do coset, conforme foi visto em (3.10).

3.3 PECODIFICAÇAO POR BUSCA SISTEMÁTICA

Vimos na seção anterior que a síndrome associada a uma n-upla Cr) é um vetor de (n-k) componentes,de modo que o número total de síndromes distintas é **Í**ⁿ ^ . Este fato,juntamente com as propriedades do arranjo padrão de um código linear (Teoremas 3.1 e 3.2) nos leva a concluir que existe uma correspondência biunívoca entre síndromes e "cosets". Escolhendo para "coset leaders" as configurações de erros [1] mais prováveis, i.e.,as de menor peso, para um canal binário' simétrico, ê possível estabelecer um procedimento para decodificar códigos lineares binários em bloco que consiste em:

T

19 -"Calcular a síndrome Cr] -CH) associada â n-upla [r) recebida.

29 Encontrar o "coset leader" correspondente a esta síndrome, ou seja, o vetor erro introduzido no canal.

39 - Somar o vetor erro â palavra recebida a fim de corrigí -la.

O procedimento descrito acima, denominado decodificação por busca sistemática, é de aplicabilidade bastante limitada se o código usado não apresenta outras propriedades' a não ser a de linearidade. Isto porque sua implementação requer operação de geração e comparação envolvendo 2^ⁿ ^ (n-k)-uplas binárias (gerador -de síndromes) , uma vez que se o código corrige t erros por blocos, devemos ter

$$C_n^1 + C_n^2 + \ldots + C_n^* \leq 2^{n-k} - 1 \qquad (3\text{-}16)$$

Portanto, mesmo para códigos de comprimento moderado (i.e. n = = 100, k = 70) esta técnica de decodificação apresenta uma complexidade que a torna proibitiva (22)

3.4 O CÓDIGO DE HAMMING

Um código binário perfeito é aquele para o qual a seguinte condição se verifica:

$$C_n^1 + C_n^2 + \ldots + C_n^{fc} = 2^{(n-kl} - 1 \qquad (3.17)$$

Os únicos códigos binários perfeitos não triviais existentes, são o código de Hamming e o código de Golay (32)

Examinemos mais detidamente a expressão (3.10) que pode ser reescrita como

$$CS)^T = CH)\ íe)^T, \qquad (3.18)$$

isto e,

$$CS) \quad \begin{vmatrix} h_{11} & 12 & h_{ln} \\ {}^{h}21 & -\backslash^{+} \ ^{\wedge}22 & e_2 + \ .2n \\ h_{(n-k)l} & h_{(n-k)2} & h_{(n-k)n} \end{vmatrix} \qquad (3.19)$$

ii

De (3.19) vê-se que um código linear binário em bloco é capaz de corrigir todas as configurações de um erro, se as colunas de sua matriz de teste de paridade são todas distintas e não nulas. Nesse caso, uma palavra recebida com um digito afetado resultará em uma síndrome não nula igual â i~esima coluna da matriz **EH**P indicando que o erro se encontra na i^esima posição Sendo assim, a matriz **(H)** de um cõdigo cuja distância mínima' ê d deve ter (d-1) colunas linearmente independentes Como **CH)** tem (n-k) linhas, para que seja possível a correção* de qualquer-erro- isolado,-o.número de colunas deve ser igual a 2 - 1, o que da origem a um. código C(n,k,d), onde

$$n - 2^c - 1 \qquad \text{C3,20.al}$$

$$k = n\text{-}c = 2^c - c - 1 \qquad \underline{\text{C3.2Q.bl}}$$

$$d = 3 \qquad \text{(.3.20.cl}$$

O cõdigo descrito acima foi introduzido em 1950 por Richard Hamming em um artigo pioneiro sobre códigos corretores de èr-ros ^ ^. Hamming propôs que a i-êsima coluna correspondesse â representação binária do decimal i. Dessa forma a conversão[1] para decimal da (n-k)-upla correspondente â síndrome indicava a posição em que se encontrava o erro. Vejamos um exemplo.

EXEMPLO 3.1 - 0 código (7,4,3) de Hamming -ê aquele cuja matriz **(H)** é

$$\{\mathbf{H}) = \begin{matrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{matrix}$$

Para uma palavra código Cfc^ k-$_2$ c_1 c_ c_3 l as equações de paridade, sao

$$_{c\,l} = K_2 + K_3 + K_4.$$

$$C- = K. + K_3 + K_4$$

$$C_3 = K + K- + K_4$$

Assim, se a palavra código transmitida (1 0 1 0 1 0 l]é recebida como (1 0 1 0 1 0 0], isto é, com um erro na sétima posição (C_3) / então:

$$(S) = Cr]\ £H^T]$$

$$CS] = (1\,0\,1\,0\,1\,0\,0\}\begin{vmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{vmatrix} = (1\ 1\ 1]$$

indicando portanto ura erro na sétima posiçao.

A eficiência do código de Hamming é dada por

$$R = {}_n \qquad \frac{2" - c - 1}{2^c - 1} = 1 - \frac{}{2^c - 1} \qquad (3.21)$$

ou

$$R = 1 - \frac{n-K}{n-k} \qquad \text{C3-22)}$$

de modo que os códigos de Hamming longos tem uma eficiência[1] que se aproxima da ideal.

Embora o código descrito acima tenha surgido pela primeira vez na literatura no clássico artigo de Shannon, em 1948, a orientação dada por Hamming foi inteiramente original. Portanto, é a ele que se deve a criação de vários conceitos e de uma terminologia própria aos códigos corretores de erros. Gostaríamos de mencionar, porém, que muitos dos resultados da teoria da codificação foram descobertos primeiramente em contextos bastantes diferentes como, por exemplo, em álgebra moderna e estatística. Nesse aspecto, o espaço de tempo existente entre as descobertas dos códigos de Hamming e dos[1] *

códigos capazes de corrigir t erros por bloco representa, segundo alguns autores, mais do que uma década de pesquisa.

Estamos nos referindo a códigos de estrutura semelhante[1] aos códigos de Hamming como, por exemplo, os códigos BCH.

CAPITULO XV

' PECOPIFICAÇÃO. PROBABTLTST1CA

Desde o surgimento dos trabalhos de Ehannon sobre a teoria da informação tem havido um crescente interesse no desenvolvimento de sistemas de comunicações eficientes, confiáveis e de fácil implementação. Sendo uma abordagem eficaz para o problema da confiabilidade, os códigos corretores de erros têm sido responsáveis por uma grande quantidade' de pesquisa nas duas últimas décadas. Teoremas e técnicas de implementação sofisticadas tem sido desenvolvidas para este [1] tipo de códigos, as quais,em geral, assumem a existência de canais com saída binária. Assim, a maioria dos detetores existentes consiste basicamente de um :demodulador analógico seguido por- um decodificador digital que opera sobre os dígitos binários produzidos pelo demodulador (FIG.4.1).

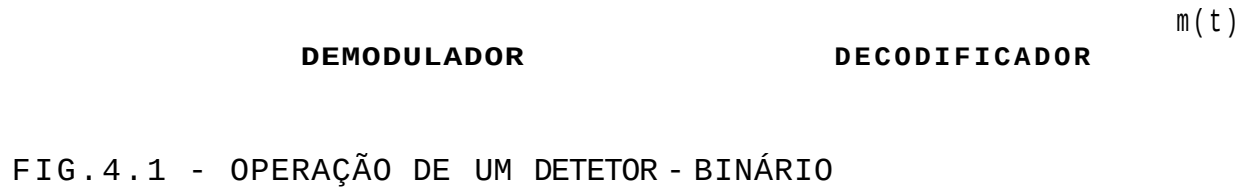


FIG.4.1 - OPERAÇÃO DE UM DETETOR - BINÁRIO

O bloco demodulador atua como um quantizador de apenas um limiar de referência. Isto significa que de acordo com: o valor da amostra que ê colhido (acima ou abaixo do limiar) um dígito binário correspondente (0 ou 1) ê entregue ao decodificador. Dessa forma a informação probabilística, potencialmente* útil, entregue ao demodulador e inteiramente destruída, o que reduz substancialmente a eficiência do sistema de comunicação(31)

O processo de deteção (demodulação e decodificação) que utiliza a informação probabilística associada â mensagem recebida, de modo a obter uma melhor estimativa da mesma, é chamado DECISÃO SUAVE. A idéia é fornecer ao decodificador informação.sobre-a^confiabilidade dos dígitos[1] recebidos, evitando assim a degradação dos sistemas de comunicação que utilizam uma quantização de apenas duas regiões, antes da decodificação. As duas técnicas de decodificação mais conhecidas, que usam decisão suave e são õtimas no sentido de minimizar a probabilidade de erro por palavra, quando as palavras código são equiprovãveis, são a decodificação por correlação de códigos em bloco e o método de Viterbi para decodificação de códigos convolucionais. Entretanto, estes sistemas ' apresentam certa complexidade de implementação, a qual só permite sua utilização para códigos 'de comprimento pequeno, devido as dificuldades de realização das operações de correlação' e armazenamento. Por este motivo, tem havido um crescente interesse nos últimos anos em esquemas de decodificação que usam decisão suave, que possam ser aplicados a códigos de alta eficiência.

Neste capitulo faremos uma descrição geral da decodificação probabilística de códigos lineares. Um algorítmp ótimo e apresentado, sendo estudado seu desempenho quando de sua utilização com códigos cíclicos. Alguns algorítmos mais simples são também discutidos, os quais, embora sub-õtimos, representam uma considerável melhoria em desempenho em relação aos sistemas que utilizam quantização binária.

4.1 DECISÃO SUAVE

O conceito do que chamamos decisão suave pode ser entendido com o auxílio da figura 4.2 abaixo.

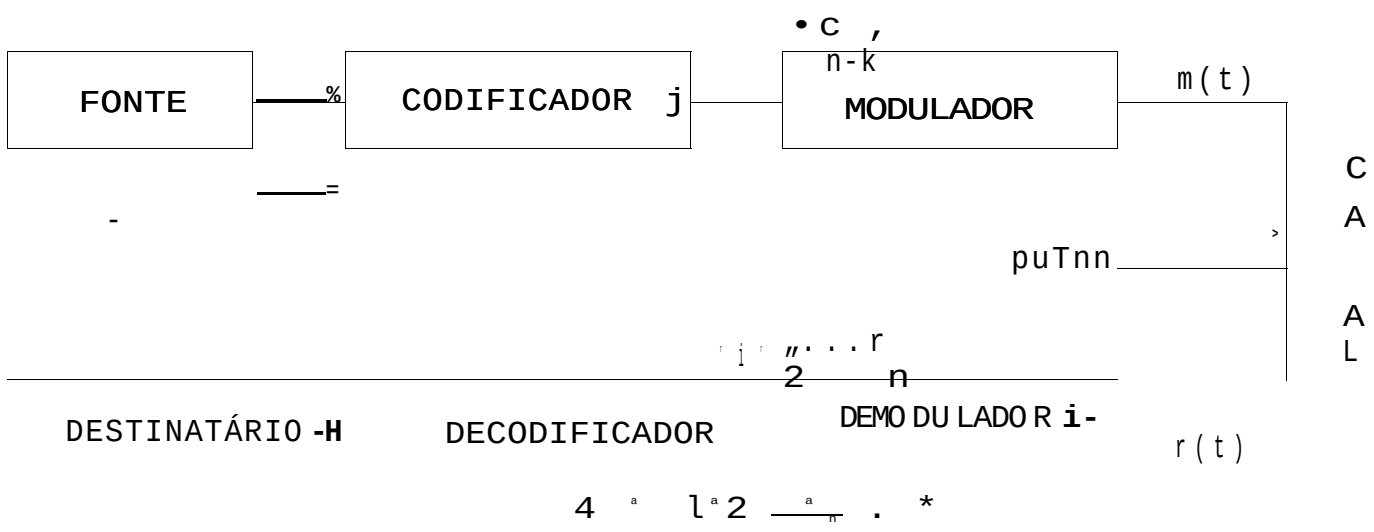


FIG. 4.2 - SISTEMA DE COMUNICAÇÃO COM DECISÃO SUAVE

Cada sequência de k dígitos binários de informação (m_1 m- . . . .m_k) é codificada em um bloco de n dígitos ($m^{\wedge}$ - - .$m^{\wedge}$ $c^{\wedge}$'. . .$_{n-k}$ y_3 r o qual é entregue a um modulador que daí gera uma forma de onda m(t) a ser transmitida. Na recepção quando o processo de decisão envolve apenas dois níveis de quantização ("hard ãecision"), o demodulador entre-

ga uma sequência de n dígitos ao decodificador. O método ' chamado DECISÃO SUAVE consiste em se ter, na saída do demodulador, além da sequência binaria de comprimento n uma se- - quência de n números positivos (a^a2---a_n) os quais forne cerão informações sobre a confiabilidade relativa dos dígitos r.- Dessa forma, se $^{a}{}_{e}{}^{>a}{}_{m}$ ' ^{0} decodificador considerará que r tem mais chances de estar correto que r . Isto pode ser feito se a saída do demodulador da figura 4.2 ê quantizada em Q níveis de modo que a estimativa do dígito binário recebido é dada pelo "byte" de decisão- suave

$$Cr.\ a.] = Cr.\ a..\ a._{\_}..\ .a. \quad] \qquad (4.1)$$

conde Q = *2^* .A confiabilidade do dígito r ^ pode ser definida através do "byte" de comprimento (J - 1)

$$Ca\ ] = Ca.,..'\langle\rangle\ .\quad 1 = \begin{cases} {}^{ca}\mathbf{ii}\text{----}{}^{a}\mathbf{iij}\text{-}\mathbf{D}^{5}\text{'} & {}^{se\ r}\mathbf{i}\ {}^{=\ 1} \\ & \text{se } r_i.\ = 0 \end{cases}$$

Portanto, a confiabilidade de um dado dígito pode variar desde C) = OO 0...03, que representa a mais baixa confiabilidade até Ca) = (11.-.13, que representa a confiabilidade máxima.

Para esclarecer melhor os conceitos [1] introduzidos nesta seção, vamos considerar um exemplo de um demodulador que quantiza a região (-A/2, + A/2) em 8 ní - veis distintos, de modo que $2^J = 8$ e $J = 3$ (FIG.4.3)

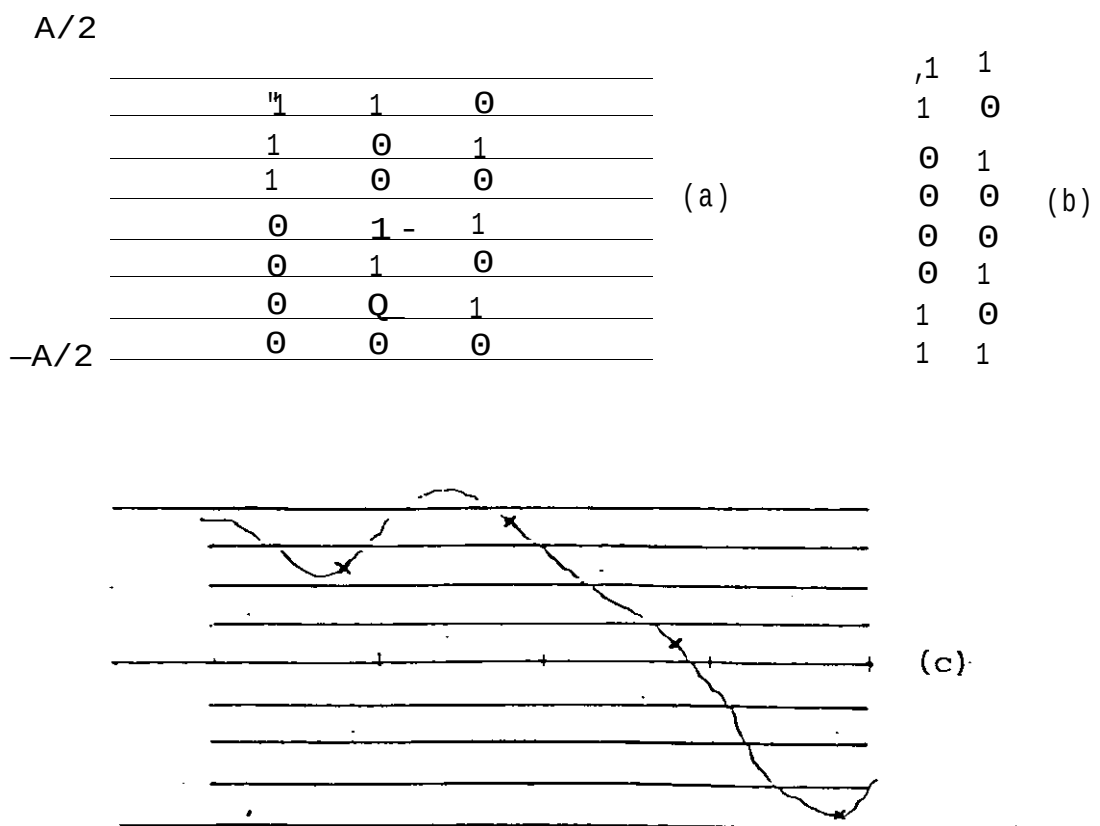


FIG.4.3 - DEMODULADOR DE DECISÃO SUAVE

a-REGIÕES DE QUANTIZAÇÃO

b-NÍVEIS DE CONFIABILIDADE

c-SINAL RECEBIDO -

Sendo assim, a salda do demodulador correspondente ã forma de onda de entrada da figura (4-3c] seria a sequência binaria 1(10)1(11)1(00)0(11}. Os "bytes" de comprimento dois entre parentesqs representam as confiabilidades dos dígitos de (1110). Note que o terceiro 1, a partir da esquerda, ê o dígito de mais baixa confiabilidade, de modo que se neste bloco de comprimento 4 o decodificador deteta a presença de um erro, este dígito de mais baixa confiabilidade ê o que mais chances tem de estar errado. Na verdade, este resultado se baseia nas propriedades estatísticas do ruído e no comportamento monotonicamente decrescente com t da probabilidade de ocorrência de t erros por bloco, em um canal binário simétrico (f 18). Neste caso, isto quer dizer que nao se pode afirmar se o terceiro dígito era 1 ou 0 originalmente, com a mesma segurança que se pode fazê-lo para os outros três. Este fato ê indicado pelo "byte" de confiabilidade, o qual localiza assim a posição mais-provável em que se encontra o erro.

Através do exemplo acima pode-se ver que, se este esquema de decisão suave é usado juntamente com um código detetor de erros capaz de detetar 1 erro por bloco (d = 2), ele permite estender esta capacidade tornando possível a correção de 1 erro por bloco. Em média, a capacidade de correção de um código pode ser duplicada quando se utilizam demoduladores de decisão suave. Isto se deve ao fato de que os (d — 1) erros detetados podem agora ser localizados através de suas informações de confiabilidade. Esta afirmação pode ser melhor visualizada com o conceito de dis —

tância suave. Introduzido a seguir-

DEFINIÇÃO 4:1 -

A distância suave entre duas n-uplas binárias u e v é a soma das distâncias, expressas em níveis , entre seus dígitos. Considerando que a distância entre níveis adjacentes ë igual a 1, tem-se

$$d_s = dCQ - 1) \tag{4.2}$$

onde d representa a distância de Hamming entre u e v.

A capacidade de correção e/ou.deteção de erros de -nível de um código, pode -agora ser estabelecida de maneira análoga â que foi feita no capitulo 2. Se d repre - senta a distância.mínima de um código linear então, em termos de decisão suave,as palavras código distam entre sí de no mínimo

$$d_s = d(Q - 1) , \tag{4.3}$$

o que permite a correção de t erros de nível por bloco onde

$$t_s < \frac{}{2} - \tag{4.4}$$

Para fixar idéias consideremos o código de Hamming (7,4,3}

capaz de corrigir 1 erro por bloco, e uma quantização de 8 níveis. Neste caso

$$d - d(Q - 1) = 21$$

e

$$t_s \leq 10$$

Como a quantidade de erros de níveis de quantização mínima ne cessaria para provocar uma interpretação errônea no demodulador é Q/2 , vemos que as configurações mais prováveis de ^ erros, que correspondem a 8 erros de nível, podem ser corrigidas, o que duplica a capacidade de correção do código.

A utilização de mais de duas regiões de quantização ê uma tentativa de se diminuir a perda de informação que resulta quando Q ê igual a 2. Portanto o detetor ' ótimo, isto é, aquele que no processo de decisão retém toda a informação contida no sinal recebido, seria aquele que entregaria ao decodificador o valor exato das amostras colhidas , precisando portanto de um número infinito de níveis de quantização. Este limite de desempenho quando comparado com o sistema que não usa decisão suave, representa um ganho em potên - cia de aproximadamente 2db [1] . Entretanto, este ganho que se pode conseguir com o aumento do número de níveis, significa um crescimento na complexidade- dos circuitos detetores

(31)

Observa-se entretanto que, a medida que o valor de Q aumenta, o ganho incremental em relação sinal/ruído para-se obter uma dada probabilidade de erro, é cada vez menor, de modo que

grande parte da degradação que ocorre quando Q vale 2 pode[1] ser superada sem que a complexidade do sistema se torne proibitiva.

4.2 - DETEÇÃO POR ZONA NULA

A forma mais simples de decisão suave[1] ê aquela que utiliza apenas três regiões de decisão, conforme mostra a fig 4.4.

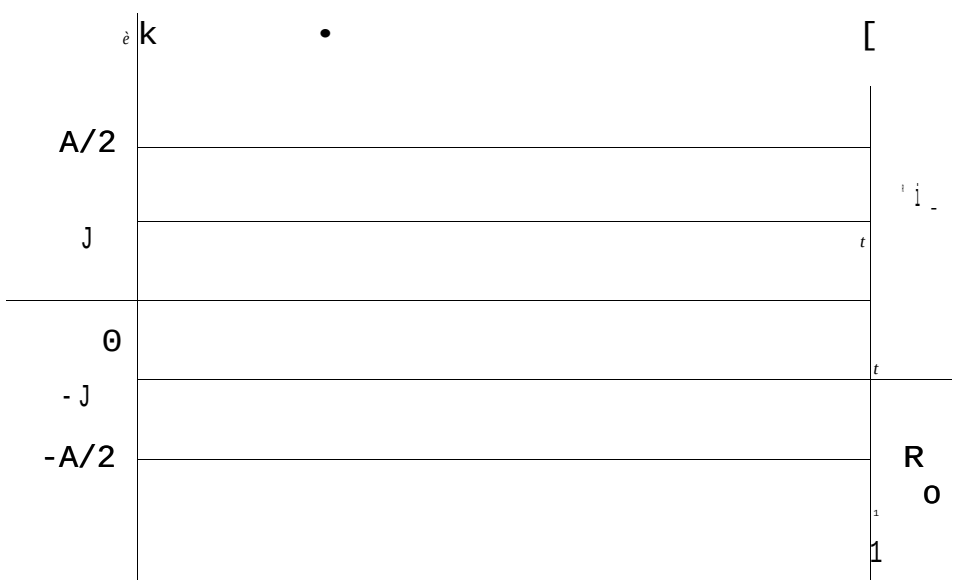


FIG. 4.4 - DETEÇAO* POR ZONA NULA - REGIÕES DE QUANTIZAÇÃO

Dessa forma o sinal recebido

$$y(t) = m(t) + n(t)$$

ë detetado, no instante t-Q , como sendo

1 , se Y(t₀) **E**R (4.5a)

X , se y(t₀) c l ^ (4.5b)

0 , se y(t₀) **E,R** (4.5c)

onde as regiões R_0, R^ e R^ são definidas por

R_0 = {y ᴇ R I y > J) (4.6a)

$R_{\blacksquare}$ ='{y **E R** | - J < y < J) (4.6b)

R = íy **E R** I y < - *3}* (4.6c)

Em (4.5b) X é um valor próximo â linha de decisão binária e portanto de valor duvidoso uma vez que as probabilidades de transição P(X | 0) e P(X | 1) tem valores próximos-Assim, guando o valor da amostra colhida situa-se na região R^, o detetor nada decide sobre ele. Nesse caso., diz-se que um nulo foi detetado. Este esquema de decisão suave e conhecido como deteçao por zona nula e representa um considerável ganho em termos de probabilidade de erro (ou da taxa de informação transmitida) sobre o sistema de decisão de apenas duas regi - — (31) ~

oes - O diagrama das probabilidades de transição de um sis_ tema que utiliza deteção por zona nula é mostrado na fig. 4.5, onde é suposto que P(l | 1)> P(0| 1)

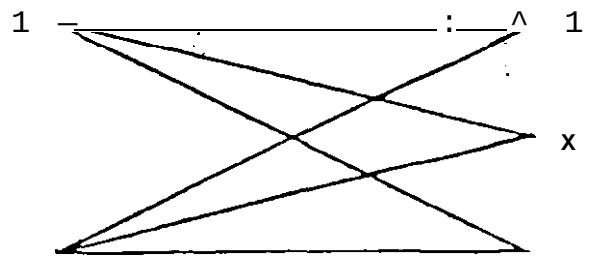


FIG.4.5 - DETEÇAO POR ZONA NULA - PROBABILIDADES DE TRANSIÇÃO

Neste trabalho vamos considerar que o ruído existente no canal se comporta como uma variável aleatória Gaussiana, de valor médio zero e variância o , conhecida. Isto quer dizer[1] que, se amostrarmos o ruído n(t) em um instante de tempo t qualquer, a probabilidade de que o valor medido esteja entre n e (n + dn) e dada por (34) f(n) dn , onde

$$f(n) = \frac{1}{\sigma\sqrt{2\pi}} e^{-n^2/2\sigma^2} \quad (4.7)$$

Este modelo do ruído aditivo é, em muitas aplicações, uma representação válida das perturbações reais em sistemas de comunicaçao.

Devido â simetria das regiões de quantização (estamos supondo que 0's e 1's sao transmitidos com igual probabilidade), são válidas as seguintes relações entre as probabilidades de transição:

$$P(0|1) = P(1|0) \quad (4.8a)$$

$$P(X|1) = P(X|0) \quad (4.8b)$$

$$P(1|1) = P(0|0) \quad (4.8c)$$

"Os símbolos X que são gerados num receptor aue utiliza esta técnica de decisão suave, representam a informação de confiabilidade fornecida pelo canal. Para utilizá—1os no sentido de produzir uma melhor estimativa da pala-

vra recebida, devemos considerar se o sistema em questão uti-liza, ou nao, codificação de canal. Na próxima seção explora-remos estas duas possibilidades.

4.2.1 - SISTEMAS SEM CODIFICAÇÃO -

A probabilidade de erro em um sistema que emprega duas regiões de decisão pode ser determinada como a seguir é descrito. Assumindo que pulsos binários de amplitu-des ± A/2 sao transmitidos em presença de ruído Gaussiano, a forma de onda v(t) sobre a qual o detetor'opera é uma varia vel aleatória cuja função densidade de probabilidade e do t i -po:

$$f_{o}(v) = \frac{e^{-(v+A/2)^2/2\sigma^2}}{\sigma\sqrt{2\pi}}$$ se um 0 foi transmitido (4.9)

$$f(v) = e^{-(v-A/2)^2/2\sigma^2}$$, em caso contrário (4.10)

O detetor incorrerá em erros sempre que acontecer

$$v(t) - + n(t) < 0 \qquad (4.11a)$$

ou

$$v(t) = - -4- -f\, n(t) > 0 \qquad (4.11b)$$

As probabilidades de ocorrência de 4.11a) e (4.11b] denominadas respectivamentes P_{el} e P^, podem ser calculadas por

$$,_x = \text{Prob}\,(v(t)<0) = \int_0^{\infty} f_x(v)\,dv \qquad (4.12)$$

$$P_{eQ} = \text{Prob}\,(_v(t)>0) = \int_0^{\infty} f_Q(v)\,dv$$

P_{e_1} e P_{e0} estao indicados na figura 4.6

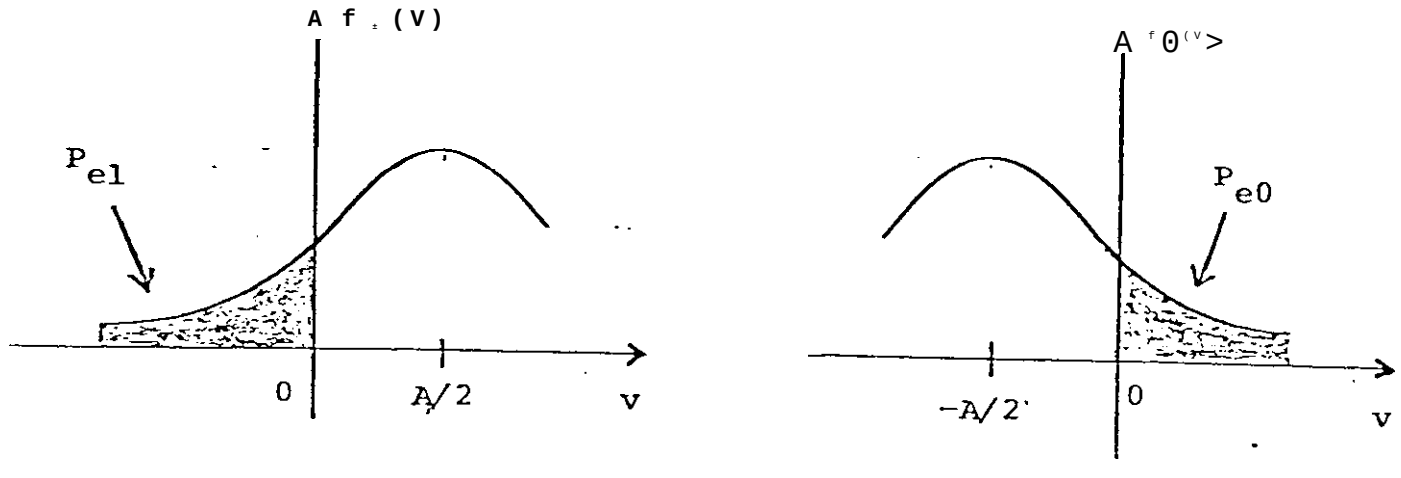


FIG.4.6 PROBABILIDADES DE ERRO EM UM RECEPTOR BINÁRIO

A probabilidade total de erro no sistema é dada por

$$e \quad 1 \quad el \quad o \quad eo \qquad (4.13)$$

onde F_1 e P_0 sao respectivamente, as probabilidades de transmissão dos símbolos 1 e 0- Admitindo que os mesmos tem igual chance de ocorrer/, então

$$e = \int_{0}^{} f_1(v)\,dv + \int_{0}^{} f_0(v)\,dv \qquad (4.14)$$

ou

$$e = \frac{1}{\sigma\sqrt{2\pi}} \int_{0}^{} e^{-(v-A/2)^2/2\sigma^2}\,dv + \int_{0}^{} e^{-(v+A/2)^2/2\sigma^2}\,dv \qquad (4.15)$$

fazendo a mudança de variável

$$x = \frac{(v + A/2)}{\sigma}$$

e possível chegarmos a

$$e = \frac{1}{2}\,erf\left(\frac{A}{\sigma\sqrt{2}}\right) \qquad (4.16)$$

onde

$$erf(x) = \frac{2}{\sqrt{\pi}} \int_{0}^{x} e^{-y^2}\,dy$$ ë chamada função erro de x

Vê-se gue a probabilidade de erro depende somente da relação sinal/ruído A/σ do sistema. em função de A/σ é traçada da na figura *4.1*

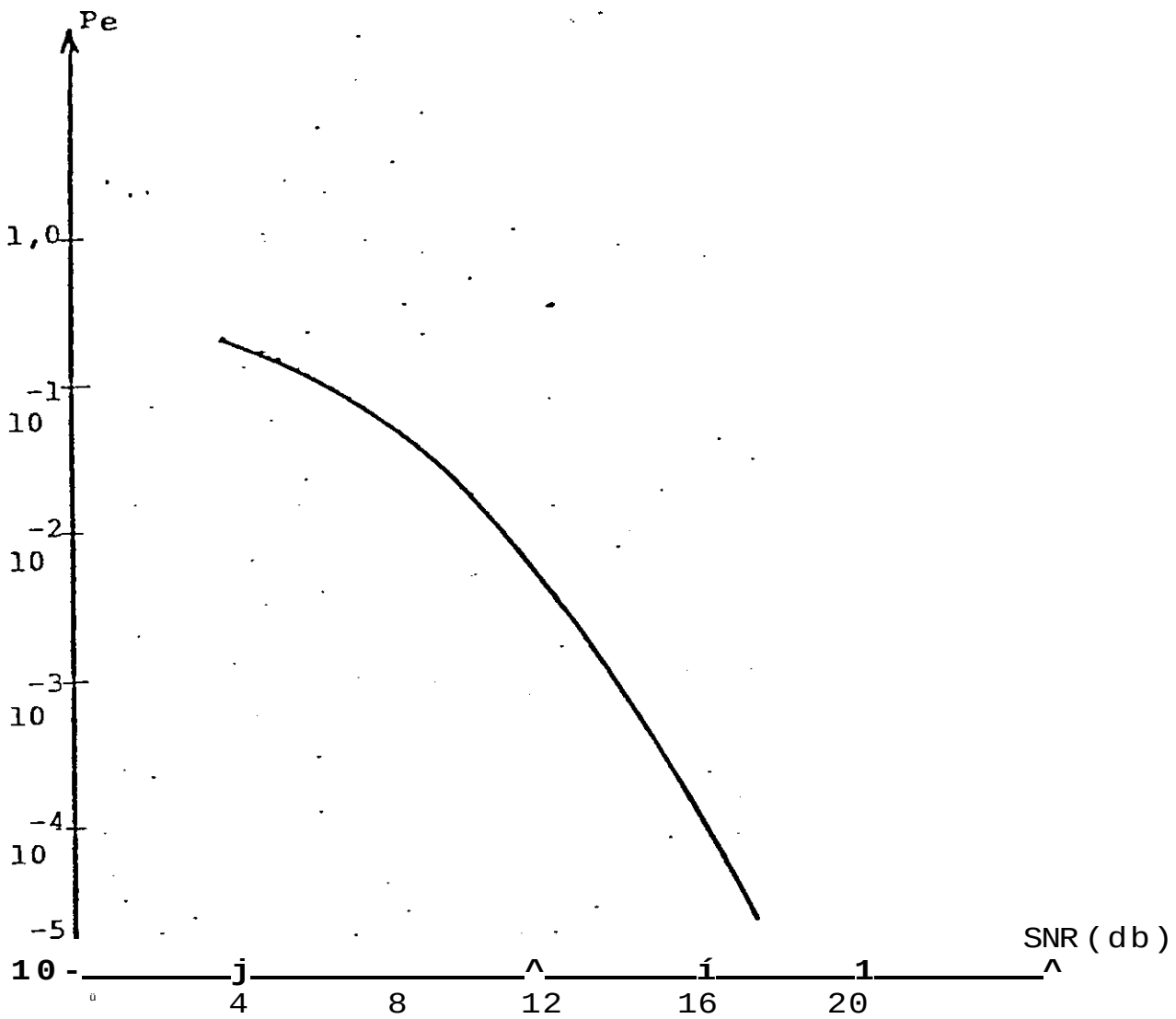


FIG.4.7 - PROBABILIDADE DE ERRO EM FUNÇÃO DA RELAÇÃO SINAL/RUÍDO PARA DETEÇÃO BINARIA EM PRESENÇA DE RUÍDO GAUSSIANO

Assim, para uma relação sinal ruxdo de 16,4 db, P_e vale 10^{-4}, o que significa, em média, um dígito detetado erroneamente em cada 10^{4} transmitidos. Existem em funcionamento diversos sistemas de comunicação onde a taxa' de erros tolerável é <10"^ , o aue requer uma reiação sinal/ruído superior a 18 db. Vejamos aoora como este valor pode ser reduzido através da detençao por zona nula.

Em um sistema de comunicação que usa decisão suave sem codificação de canal, torna-se necessária a existência Qe um canal de realimentação, para que a informação de confiabilidade possa ser aproveitada. Através deste canal são enviadas as solicitações para repetição dos dígitos detetados como nulos. Para ilustrar o cálculo da probabilidade de erro consideremos a figura 4.8, onde J define a região nula de deteçao-

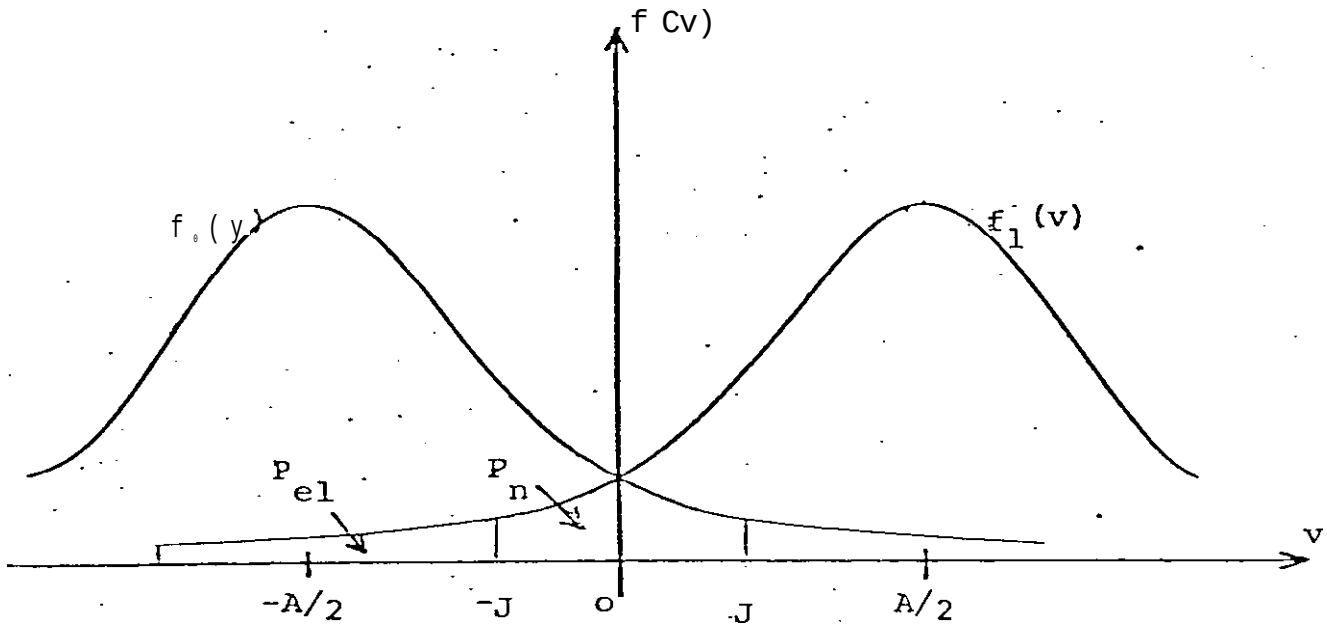


FIG. 4.8 - Deteçao por zona nula - Probabi1idades de erro

P , agora,é a probabilidade de que. o sinal recebido (pulso de amplitude ± A/2 mais ruído) tenha' um valor abaixo de + J . Se P representa a probabilidade de aue o sinal recebido esteja na regiao nula, a probabilidade de erro, se o 1 for transmitido, é a soma das probabilidades de que [1) a amostra recebi

da tenha um valor menor que $-J_t$, (2) a amostra situe-se na região nula e a retransmissão tenha um valor menor que $-J$, (3) a amostra e a 1ª retransmissão situem-se na zona nula e a 2ª retransmissão tenha um valor menor que $-J$, e assim sucessivamente.

Logo

$$P_e = P_{el} + P_n P_{el} + P_n^2 P_{el} + P_n^3 P_{el} + \cdots \qquad (4.17)$$

ou

$$P_e = \frac{P_{el}}{1-P_n} \qquad (4.18)$$

O número médio de transmissões efetuadas até que o detetor tome uma decisão (correta ou nao) ê dado por

$$N = (1-P_n) + 2P_n(1-P_n) + 3P_n^2(1-P_n) + \cdots \qquad (4.19)$$

$$N = (1-P_n)\sum_{j=1}^{\infty} j P_n^{j-1} = (1-P_n)\sum_{j=1}^{\infty} \frac{d}{dP_n} P_n^j$$

$$N = (1-P_n)\frac{d}{dP_n}\sum_{j=1}^{\infty} P_n^j$$

$$N = (1-P_n)\frac{d}{dP_n}\left(\frac{1}{1-P_n}\right)$$

$$N = \frac{1 \cdot}{1 \sim P_n} \quad (4.20)$$

Combinando (4.18) e (4.20) podemos escrever

$$P_e = N P \quad (4.21)$$

Para se ter uma idéia quantitativa do que é possível obter com a zona nula, consideremos que a probabilidade de erro sem a mesma é 10^ (figura 4.7), o que requer uma relação sinal/ruído de 18 db. O deslocamento do nível de decisão de zero para ±J/2 é equivalente, em termos de probabilidade de erro, a manter o mesmo em zero e reduzir A de J unidades. Para *J/a* igual a 2 db tem-se

$$A - J_{db} = 16 \; ' * P_n = 10^4$$

$$' R" = \frac{1}{1 - P_n} = 1{,}0001$$

$$- \quad * \quad 4$$

de modo que em media, apenas um digito binário em 10 precisa ser repetido. Para calcular o efeito sobre a probabilidade de erro lembremos que uma zona nula de largura J equivale a manter o limiar de decisão em zero e aumentar A de J unidades. Então:

$$P_e = \frac{1}{2}\left[1 - \mathrm{erf}\left(\frac{A+J}{2\sigma\sqrt{2}}\right)\right] = \frac{1}{2}\left[\mathrm{erfc}\left(\frac{A+J}{2\sigma\sqrt{2}}\right)\right] \qquad (4.22)$$

onde

$$\mathrm{erfc}\ (x] = 1 - \mathrm{erf}\ (x)$$

é a função erro complementar de x. Para $A/\sigma >> 1$, podemos usar a expansão assintótica para erfc (x)

$$\mathrm{erfc}\ (x) \_ \frac{e^{-x^2}}{x\ 11} \qquad x \gg 1 \qquad (4.23)$$

de modo que

$$P_e = \sim \frac{e^{-(A+J)^2/8\sigma^2}}{\qquad\qquad} \qquad (.4.24)$$

Para $A + J$ = 20 db, obtém-se

$$P_e = 0{,}6 \times 10^{-6}$$

ou seja, há uma redução na probabilidade de erro em mais de uma ordem de grandeza, ao passo que a taxa de transmissão pra ticamente nao foi afetada.

4.2.2 - SISTEMAS CODIFICADOS -

£ sabido que um código com distância minima d ê capaz de corrigir t erros por bloco, onde

^ C4.25,

Em um receptor que usa deteção por zona nula antes da decodificação, esta capacidade de correção pode ser aproximadamente duplicada. A idéia é queagora o detetor entrega ao decodificador informação sobre a confiabilidade dos dígitos recebidos . Os dígitos detetados como nulos tem mais chance de estar errados. Sabendo disso, o decodificador, ao detetar a presença de erros, tem as localizações mais prováveis onde os mesmos se encontram e pode então corrigi-los. Desde que a quantidade de dígitos detetados como nulos seja < (d - 1), os mesmos podem ser corrigidos na maioria dos casos, e o código tem sua capacidade de correção aproximadamente dobrada. No caso da palavra recebida ter mais que (d - 1) dígitos de baixa confiabilidade, então o decodificador simplesmente ignora esta in - formação de confiabilidade e opera como se a quantização no ' detetor fosse de apenas duas regiões. Dessa forma, o desempenho de um receptor que usa deteção por zona nula é, no míni - mo, igual aquele que usa dois níveis de quantização apenas . Uma questão extremamente importante relativa ã utilização con junta de deteção por zona nula e codificação de canal é a escolha da abertura da janela (região nula), isto é, do limiar de decisão J. Se J é um valor de tensão muito pequeno, então poucos dígitos serão de baixa confiabi1idade, levando pouca informação ao decodificador. Por outro 1ado, se J é um va

lor de tensão muito alto, então quase todos os dígitos recebi dos serão de baixa confiabil-idade, o que não interessa ao des- codificador. De um modo ou de outro, o receptor se comporta - ria como se Q fosse igual a 2. Percebe-se então a existên- cia de um valor õtimo para J, no sentido de minimizar a pro- babilidade de erro na saída do decodificador, o qual é função da relação sinal/ruído existente e do tipo de código usado.

4.3 - PROCEDIMENTOS SUBÕTIMOS

Nesta seção descrevemos dois algoritmos ' de decodificação com decisão suave que são subÕtimos no senti do de que o ganho teórico mãximo possível de obter com este ' tipo de decisão não ê atingido. O primeiro deles, devido a Harrison^^^, utiliza o código de Hamming (7,4,3) e é descri- to a seguir.

Sabe-se que quanto maior for o número de níveis de quantização em um esquema de decisão suave, maior é a quantidade de'informação útil â qual o decodificador tem acesso. Entretanto pode ser mostrado , que a utilização de mais de 16 níveis tem pouco efeito sobre a probabilidade de erro do sistema. Como a complexidade dos circuitos detetores/ decodificadores aumenta rapidamente com o acréscimo do número de níveis Harrison analisou o desempenho de um sistema que [1] utilizava apenas 4 regiões de decisão, como mostra a figura ' 4.9, onde

FIG.4.9 - ALGORITMO DE HARRISON - REGIÕES DE QUANTIZAÇÃO

H e L representam as regiões de alta e baixa confiabilidade[1] respectivamente. Vimos; no cap. -3 que a síndrome de uma "pala – vra recebida é igual a i–ésima coluna da matriz H se um erro ocorreu na posição i. Todavia, se dois dígitos estão errados, a síndrome indica a ocorrência de um erro em uma terceira posição, que está correta, e ao tentar corrígi-la, o decodificador introduz um outro erro na palavra. Este efeito pode ser dimi - nuído quando se usa decisão suave, fazendo-se com que 'o decodificador tente corrigir somente as posições de baixa confiabilidade. Ò procedimento de Harrison consiste basicamente dos se - guintes passos:

1 - Se a palavra recebida possui 0,1 ou mais que dois dígitos' de baixa confiabilidade então o decodificador~atua normalmen – te, como se não tivesse havido decisão suave na deteção.

2 - Se a palavra recebida tem dois dígitos de baixa confiabilidade, -então a síndrome da mesma é calculada e então:

a) Se S ê igual a zero então a palavra é suposta estar correta e é liberada.

b) Se S indica um erro sobre uma posição de baixa confiabilidade, então a mesma é corrigida e a palavra liberada.

c) Se S- indica um erro em uma posição de alta confiabilidade então os dois dígitos de baixa confiabilidade são invertidos e a síndrome é recalculada. Se o novo valor de S for zero então dois erros foram detetados e corrigidos. Em caso contrario ocorreu um erro em uma posição de alta confiabilidade e o decodificador-deve -operar normalmente, desprezando .a informação probabilística.

_ . As curvas de desempenho obtidas com este algoritmo para três limiares de decisão diferentes, são mostrados na figura 4.10. Observemos a existência de um valor ótimo para J entre 40/50% da amplitude dos pulsos binários transmitidos, que permitem um ganho de aproximadamente 1 db para o algoritmo proposto por Harrison.

O segundo procedimento subotimo que [1] descrevemos, devido a Farrell e Kalligeros^^utiliza um código, de um dígito de paridade, de comprimento igual a 8, e um detetor de decisão suave quantizado em 8 regiões, cujos níveis valem + Q,25V,± Q,5V e + 0,75y, para sinais de amplitude ± IV-

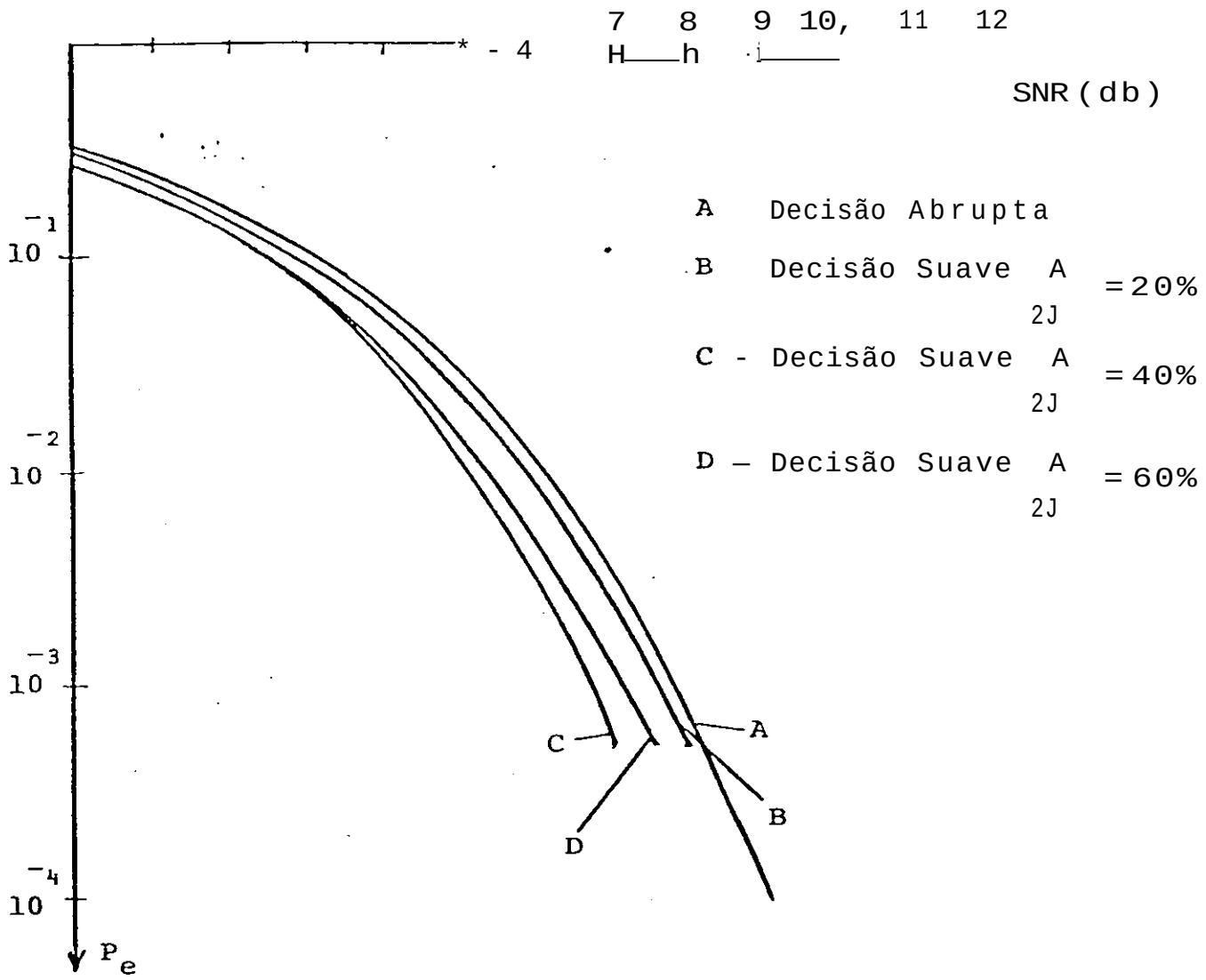


FIG. 4.10 - ALGORITMO DE HARRISON - CURVAS DE DESEMPENHO._

O algoritmo consiste basicamente dos seguintes passos:

a) Avaliar os dígitos ±2"*"'6^7 l seus "bytes" de confiabilidade.

b) Recalcular o dígito de paridade C^ a partir dos dígitos de informação e compará-lo com o valor recebido de C^.

b-1 - Se estiver correto, assumir que nao houve erros e liberar a palavra.

b-2 - Em caso contrário, inverter o digito de mais baixa confiabilidade, de modo a corrigir o erro isolado* mais provável, e liberar a palavra.

A curva de desempenho, obtida por simulação em computador, relacionando probabilidade de erro e relação sinal/ruído para este algoritmo é mostrado na figura 4.11 Para reiações sinal/ruído maiores que -2.5 db observa-se um ganho em relação ao sistema sem codificaçao, o qual é maior * que aquele obtido por um código de Hamming de mesmo comprimento e/ou eficiência.

Os procedimentos descritos acima não apresentam nenhuma propriedade de otimalidade em relação a algum critério. De fato, os limiares de decisão (abertura da janela no método de Harrison e o posicionamento dos níveis de quantização no trabalho de Farrell/Kalligeros) são estabelecidos de maneira inteiramente arbitrária, o que ê responsável, em parte, pelo desempenho subõtimo dos dois algoritmos.

Na seção seguinte abordaremos algumas investigações teóricas, baseadas em certos critérios de otimização, que levam a definição de valores ótimos para J.

4.4 - NÍVEIS DE QUANTIZAÇÃO ÓTIMOS -

A definição dos níveis de quantização em um receptor que faz uso de decisão suave é uma questão fundamental no projeto dos sistemas de comunicação que empregam es

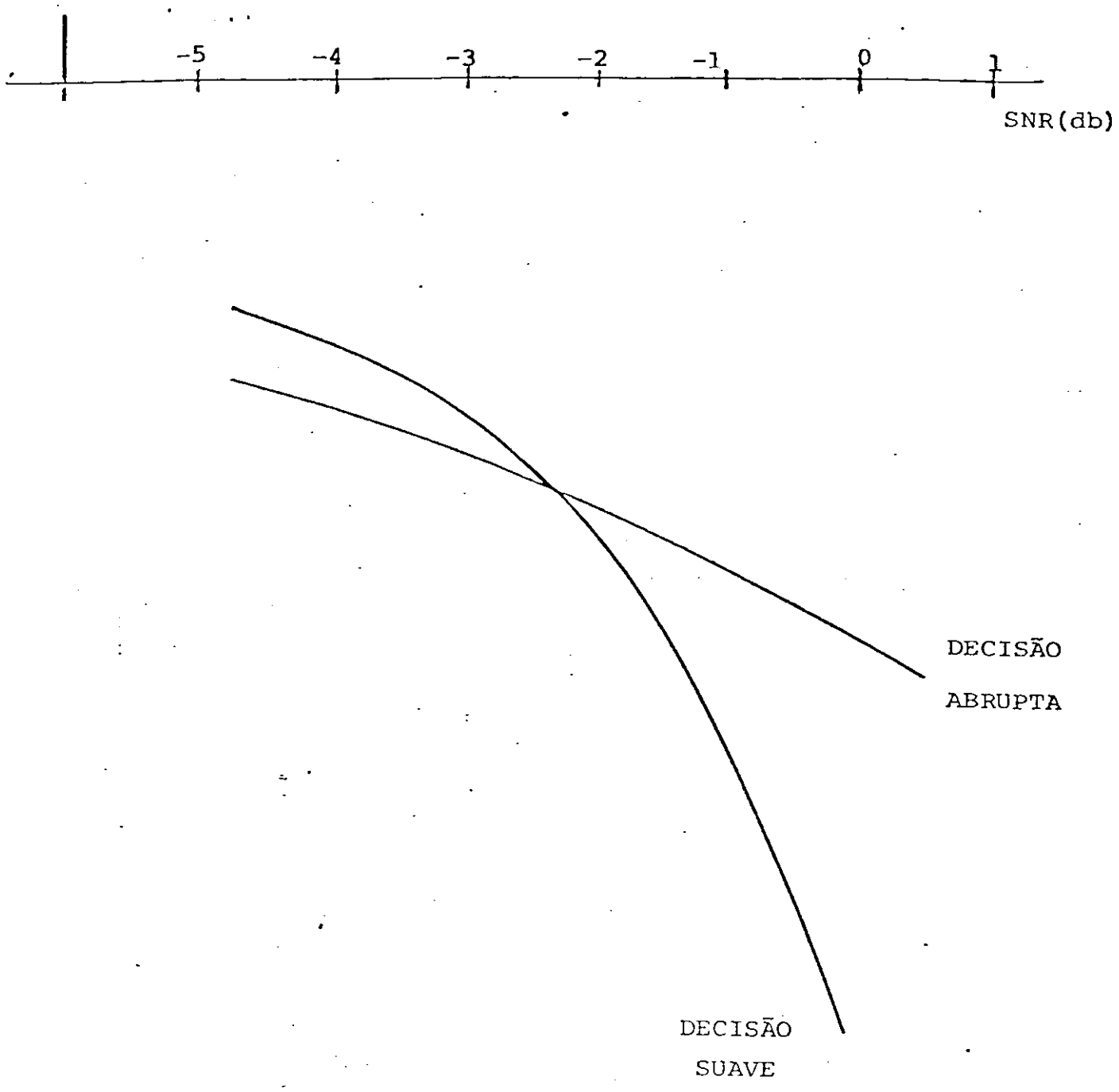
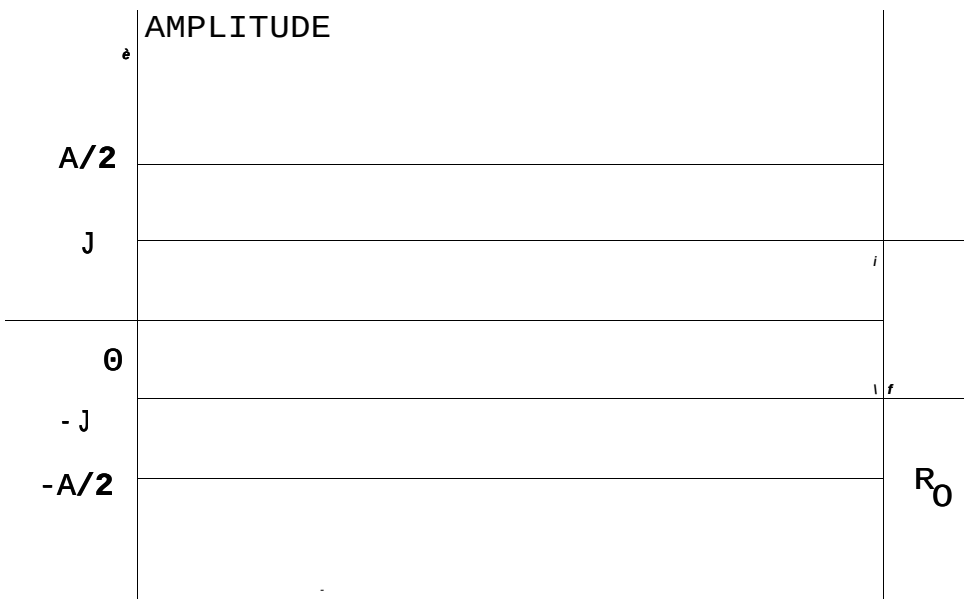


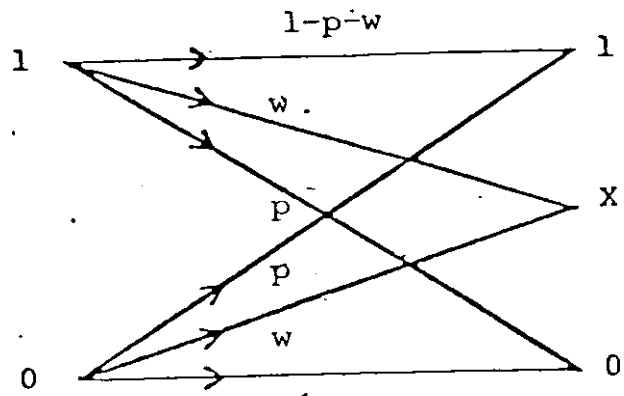
FIG.4.11 - CURVAS DE DESEMPENHO DO ALGORITMO DE FARRELL E KALLIGEROS

te tipo de deteção. Nesta seção, abordaremos este tipo de problema para ura receptor cujo espaço de sinal é quantizado em três regiões, isto ê, tentaremos encontrar o valor ótimo da abertura J, conforme a figura 4.12. Este procedimento i devido a Bloom et al (37)



FIG,4.r2 - DETEÇAO POR ZONA NULA - CÁLCULO DO VALOR ÓTIMO DE J

Inicialmente provaremos a existência de um valor õtimo para *J*, no sentido de maximizar a taxa de informação, em bits por símbolo. O diagrama de probabilidades de transição referente à figura 4.12 ê mostrado a seguir



e w sao.definidos por

$$p = \int_{a/2\sqrt{T}}^{r^{3}} e^{-(v-A/2)^{2}/2o^{2}}\, dv \qquad (4.26)$$

$$w = \int_{/2\hat{I}T}^{J} e^{-(v-A/2)^{2}/2o^{2}}\, dv \qquad (4.27)$$

$$-J$$

A taxa de informação para este tipo de canal ê dada por[3]

$$R(J) = P(l|D\log_{2}\frac{2P(lU)}{P\{1|1)+P(0|1)J} + P(0I1)\log_{2}\frac{2P(011)}{P(1|1)+P(0|1)\ \mathbf{J}} \qquad (4.28)$$

ou

$$R(J) = (1\text{-}p\text{-}w)\ \log_{2}\left|\frac{2\,Çl\text{-}p\text{-}w)}{1\ -\ w}\right| + P\ \log_{2}\left|\frac{2w}{1\text{-}V7}\right| \qquad (4.29)$$

Para mostrar que R(J) possui um máximo para algum J>0, pre

cisamos que

$$\_3K\_ \qquad ?\bullet\ 0 \qquad \text{C4-30)}$$
$$J\ \sim\ 0$$

Isto pode ser feito se escrevermos

$$P(l|l) = 1 - \int_{-J}^{J} f_n(v-A/2)dv - \int_{-J}^{J} f_n(v-A/2)dv \qquad \text{C4.31a)}$$

ou

$$P(l[lí = \int_{J-A/2}^{:-J} f_n(v-A/2)dv \int_{-J}^{J} f_n(x)dx \qquad (4.3Lb)$$

$$P.(0|1) = \int_{-J-A/2}^{J} f_n(v-A/2)dv \qquad (4.32)$$

ou

$$P(0|l) = \int_{-J}^{J} f_n(x)dx \qquad (4.33)$$

derivando (4.28) obtemos

$$R(J) = P'(1|1)\log_2 \frac{2P(1[1)}{P(l]l)+P(0|l)} + P^1(0|l)\log. \frac{2P(0\,11)}{P(l|l)+P(0|l)} \qquad (4.34)$$

onde

$$P'(1|1) = -f(J-A/2) \qquad (4.35)$$

$$P^1(0I1) = -f(J-A/2) \qquad (4.36)$$

Segue—se então que

$$.'CO] = - f_{n}C - V2] \log_{2} \frac{\bullet 4P(lll)P(Q|l)}{CP(l[l)+P(0|l)\ )} \qquad (4.37]$$

Considerando que P (l | l) > P **CO 113 r**

tem-se

$$CP(1|1) + P(0[1))^{\wedge} > 4P(l|l)P(0|l)$$

e assim $R^{1}(0] > 0$ desde que $f_{n}(-A/2] \wedge 0$. Portanto, a taxa de informação R atinge um máximo para algum valor de J>0 . No que se segue encontraremos valores õtimos para J relacionados com a figura 4.12 e determinaremos o ganho que o mesmo apresenta em relação~aos~sistemas:que~nao~usam :decisão suave.

4.4.1 - SISTEMAS SEM CODIFICAÇÃO -

O ganho que se pode ter em relação a probabilidade de erro com um esquema como o da figura 4.9 e função do tipo de ruído existente no sistema. Quando o mesmo é do tipo aditivo Gaussiano, as probabilidades de transição p e w são dadas pelas expressões (4.26) e (4.27). As probabilidades P(111-) é P(0|l) podem ser calculadas diretamente [1] com o auxilio da figura 4.13.

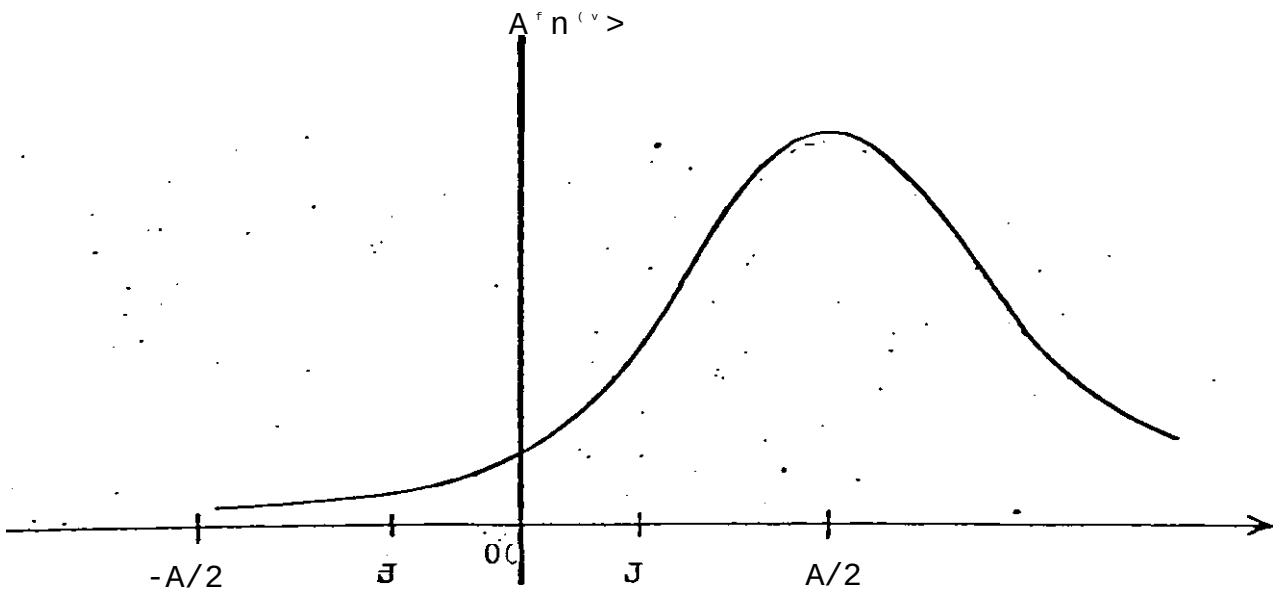


FIG.4.13 - Densidade de probabilidade de um pulso de amplitude A/2, em presença de ruído Gaussiano

Temos

$$\frac{1}{o/2II} \int_{J}^{-(v-A/2)^2/2o^2} dv \qquad (4.38)$$

ou

$$P(1|D \_ \frac{1}{/ir} \int_{J^A/2}^{'} -x^2 dx \qquad (4.39)$$

e assim

$$P(l|l) \; \_1 \quad 1 + erf \frac{/A/2 - X}{2} \qquad (4.40)$$

De maneira análoga

$$PC0|1) = \int_{-a}^{*4} \frac{-CV-A/21V_2^2}{} dv \qquad (4.41)$$

ou

$$P(0|l) = \frac{1}{\sqrt{2\pi}} \int_{-J-A/2}^{-x^2} dx \qquad (4.42)$$

$$P(0|1) = - \frac{1}{} - - (cr¥) \qquad (4.43)$$

O valor õtimo de J ocorre quando (4.34) torna-se zero e pode ser obtido com o auxílio de (4.40) e (4.43). A figura 4.14 mostra a taxa de informação R como função da relação sinal/ruído, quando J assume este valor õtimo. Para efeito de comparação apresentamos os resultados obtidos para os casos extremos de apenas duas regiões de decisão e de um número infinito de níveis de quantizaçao.

Observamos que ,com o emprego da zona nula podemos obter cerca de 50% do ganho teórico possível. Um desempenho superior a este requer um maior número de regiões de quantizaçao, porem , acima de 16 níveis o acréscimo em-ganho não justifica a complexidade dos circuitos detetores [31]

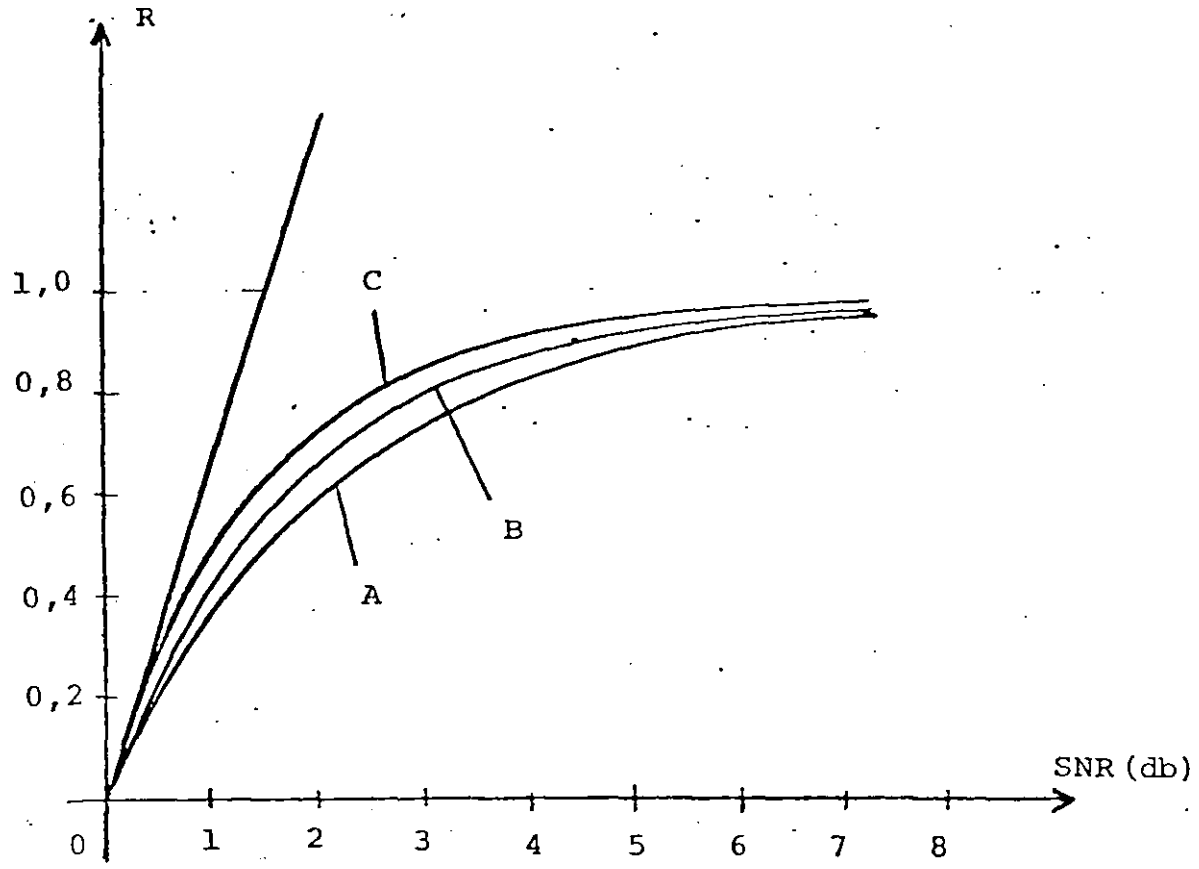


FIG. 4.14 - TAXA'DE INFORMAÇÃO COMO FUNÇÃO DA RELAÇÃO SINAL / RUÍDO

(A) DECISÃO ABRUPTA (Q=2)

(B) DETEÇÃO POR ZONA NULA

(C) Q = -

. Um aspecto importante relacionado com os nl - veis de quantização ótimos de um esquema de decisão suave é o fato de que os mesmos dependem da relação sinal/ruído do sistema, a qual nem sempre é constante. Sendo assim, ë praticamente impossível manter-se a propriedade de otimalidade de um dado nível de decisão. Para um esquema como o da figura 4.9 portanto, é importante que se analise o comportamento do sistema em relação a variações de A/o. Para se fazer isto é conveniente introduzirmos um fator N, o qual representa a am

plituâe da. janela J normalizada em relação a amplitude do sinal- Assim

N â

Na figura 4.15, obtida diretamente da expressão 4.34, está mostrada a dependência entre N e a relação sinal/ruído do sistema.

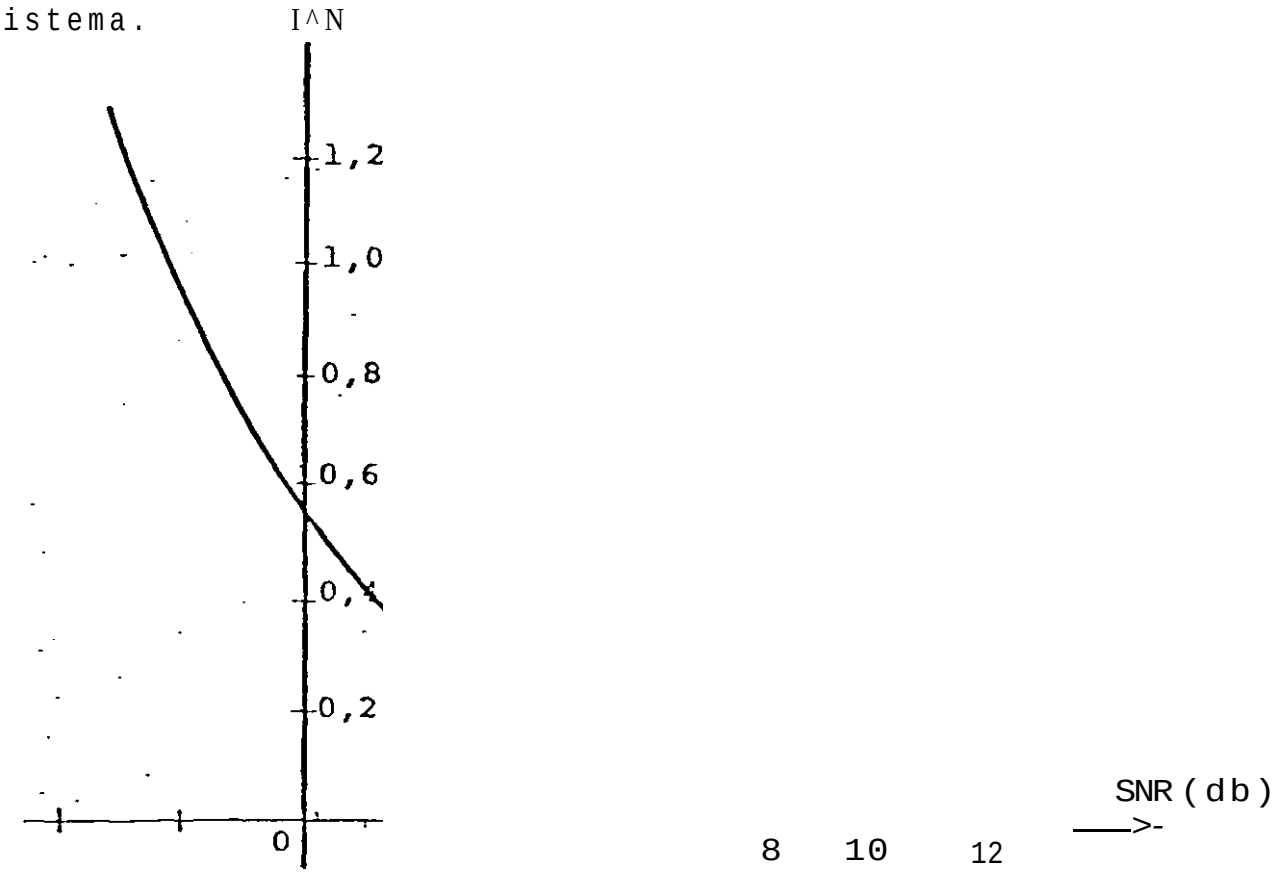


FIG-4.15 - VALOR ÕTXMO DA REGIÃO NULA EM FUNÇÃO DA RELAÇÃO SINAL/RUIDO

Se considerarmos um. valor N_q fixo, que é ótimo para uma da da relação sinal/ruldo e acontece da mesma diminuir, então N estará entre zero e o novo valor ótimo. Observando a figura 4.16, onde está mostrada a eguivocação , em função de J, para diversos valores da relação sinal/ruído, vê-se que

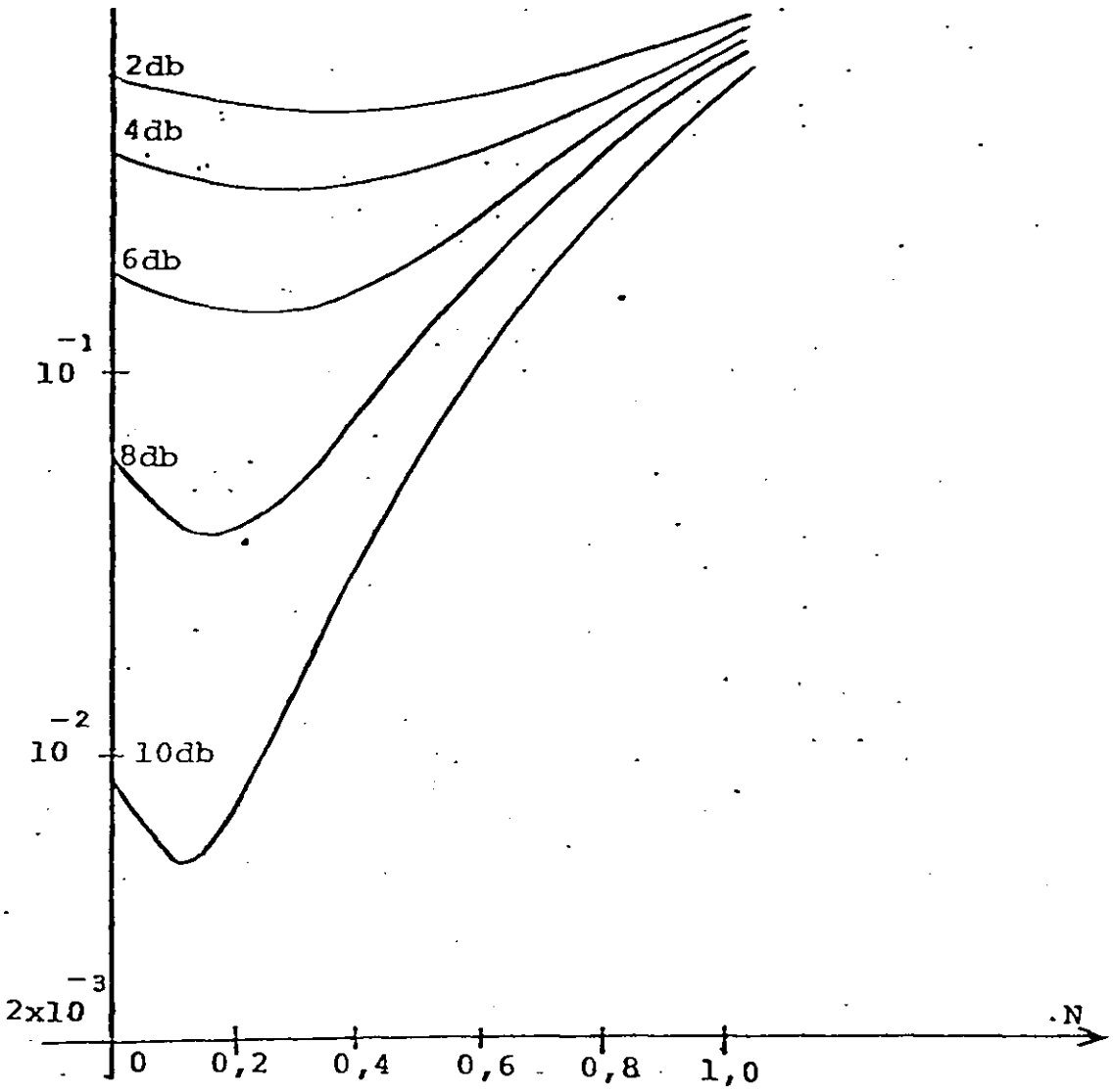


FIG.4.16 - EQUIVOCAÇÃO EM FUNÇÃO DE JS EM UM SISTEMA DE DETEÇÃO POR ZONA NULA.

para valores pequenos de A/o o sistema de deteçao por zona nula que estamos analisando tem um desempenho superior àquele que usa apenas duas regiões de decisão. Porém, o contrario acontece quando A/o aumenta. Isto acontece porque nesse caso o sistema de deteção destrói muita informação, parte da qual é de alta confiabilidade e' está disponível no esquema de dois níveis. Esta degradação em desempenho pode ser superada se o espaço de sinal é quantizado em quatro regiões e

a performance obtida, é sempre superior aos outros dois ca - sos . Observamos ainda que quajido o valor de J e aproxi- madamente duas vezes seu valor ótimo, o sistema tem um desem- penho inferior aquele que teria se Q fosse igual a 2. Esta sensibilidade em relação sinal/ruído (ou do valor õtimo de J) é uma característica negativa do sistema de deteção por zona* nula.

4.4.2 - SISTEMAS CODIFICADOS -

Veremos agora como o desempenho de um código corretor de erro pode ser melhorado se o mesmo é usado juntamente com um detetor de decisão suave. Considere – mos o código de Hamming (n,n-l,2), capaz de detetar um erro em cada bloco de n dígitos. Este é um código de um dígito * de paridade, o qual é calculado pela soma módulo 2 dos n-1 dígitos de informação. O emprego de três regiões de decisão [1] (zona nula) permite que_ p dígito de paridade . seja_jutilizado [1] não apenas para deteção-de erros mas também, em muitos casos, para correção dos.mesmos. Sempre que uma palavra recebida t i - ver um X (nulo), o dígito de paridade e usado para preen - cher esta posição e a palavra é aceita. Se q-^/pj e u^ re- presentam, respectivamente, as probabilidades de que um dígi- to transmitido seja recebido corretamente, erradamente ou co- mo um nulo, então pode—se mostrar que

$$\hat{i}_{x} = \frac{1}{2}\left[1 + \operatorname{erf}\left(\frac{A_0 - J_0}{\sqrt{2}}\right)\right] \quad (4.45a)$$

$$P_1 = \frac{1}{2}\left[1 - \operatorname{erf}\left(\frac{A_1 + J_0}{\sqrt{2}}\right)\right] \quad (4.45b)$$

$$u_x = \frac{1}{2}\left[\operatorname{erf}\left(\frac{A_0+J_1}{\sqrt{2}}\right) - \operatorname{erf}\left(\frac{A-J}{\sqrt{2}}\right)\right] \quad (4.45c)$$

onde

$$A = \frac{A}{\sigma_{2/2}} \quad (4.46a)$$

$$J = \frac{J_0}{\sigma_{2/2}} \quad (4.46b)$$

A probabilidade de que uma palavra aceita na recepção difira em r posições da palavra código- enviada é dada por

$$P_r = q_1^{n-r} + (n-r)\,q_1^{n-r-1}\,p_1\,u_1 + r\,q_1^{n-r}\,p_1^{r-1} \quad (4.47)$$

Para que isto ocorra é preciso a interpretação errada de r posições, sendo r um número par. A expressão (4.47) vem do fato de que isto pode ocorrer de três modos diferentes:

1 - Quando não existirem brancos- (x) e r erros forem cometidos.

2 - Quando um branco for recebido e preenchido corretamente, tendo ocorrido r erros.

3 - Quando um branco for recebido e preenchido erradamente,

tendo ocorrido r ~ l erros.

Para que uma palavra recebida seja aceita e la deve conter, no mãximO/Um "nulo". Assim, se g, p e u representam, respectivamente, as probabilidades de que uma palavra código recebida seja aceita corretamente, errada-mente, ou nao seja aceita, temos

$$p + q + u = 1 \tag{4.48}$$

$$P+q = \sum_{0}^{n} C^{\wedge}_{+1} P_r * r \text{ par} \tag{4.49}$$

A taxa de informação^ ^ ^ , em bits por palavra, é

$$\mathbf{R} = n(p+q) \text{ " } Cp+q) \log\text{-- } <P+q) + \sum_{0}^{n} C P_r \log P_r \tag{4.50}$$

A fim de encontrar valores ótimos para J consideremos o sis tema para valores altos de A/o , onde a probabilidade de ocorrência de mais de um erro (ou nulo) ê pequena, ou seja

$$P_Q \gg P^2 \gg P^4 \text{" } \bullet * \tag{4.51}$$

jvesse caso (4.50) torna-se

$$R = n\, Q_Q = \boldsymbol{n}\, q \tag{4.52}$$

ou

$$R = n\, Cq_a^{n+l} + (n+l)\, q^{\wedge}\, u^{\wedge} \tag{4.53}$$

diferenciando ejtj relação a. £ obtemos

$$- \quad Pi .+ nqj"^{1} <g£ u = 0 \qquad (4\text{-}54)$$

e daí

$$\frac{p i}{n \quad u \quad l \quad q \quad i} \qquad (4.55)$$

Fazendo uso das expressões (4.45), a condição de otimalidade' reduz-se a

$$e^{00} - \frac{4A J \qquad 1 + *(A - J)}{nU(A_{o+}J_{o}) - \bullet CA_{Q}-J_{0})J} \qquad (4.56)$$

Aplicando a expansão assimptõtica para a função erro (expressão 4.23) ficamos com

$$^{4A}o^{J}o \qquad 2/ITCA..-J)\bullet \ ^{(A}cT^{J}o^{)2}$$

n

e assim

$$^{4A}o^{J}o^{S\ CA}o-^{J}\wedge^{2} \qquad (4\text{-}58)$$

ou

$$N = \frac{J}{A_{o}} = 13\text{-}2/2) = 17,16\% \qquad (4.59)$$

Este valor ótimo para J representa um ganho em potência de aproximadamente 1,4 db em relação ao sistema onde Q vale* 2- Um aumento de 0,5 db sobre este resultado, pode ser conse

guido quando se usam quatro regiões de decisão, ou seja, uma zona nula dupla. A principal desvantagem do método de zona nula para sistemas sem codificação, i.e. sua sensibilidade em rela - ção a variação de J, também existe quando se usam códigos de mo do que para certos valores de J, sistemas codificados que usam decisão suave apresentam um desempenho inferior aqueles que usam decisão abrupta antes da decodificação. Na figura 4.17 mostramos a equivocação, em função da relação sinal/ruído, para diversos esquemas de deteção. Observamos que o sistema que emprega quatro regiões de decisão (zona nula dupla) tem um desempenho apenas li geiramente superior aquele que usa somente uma zona nula. Sua principal vantagem sobre este^último, está na baixa sensibilida- de, em relação a variações do nivel ótimo, que o mesmo apresen - ta.(37)

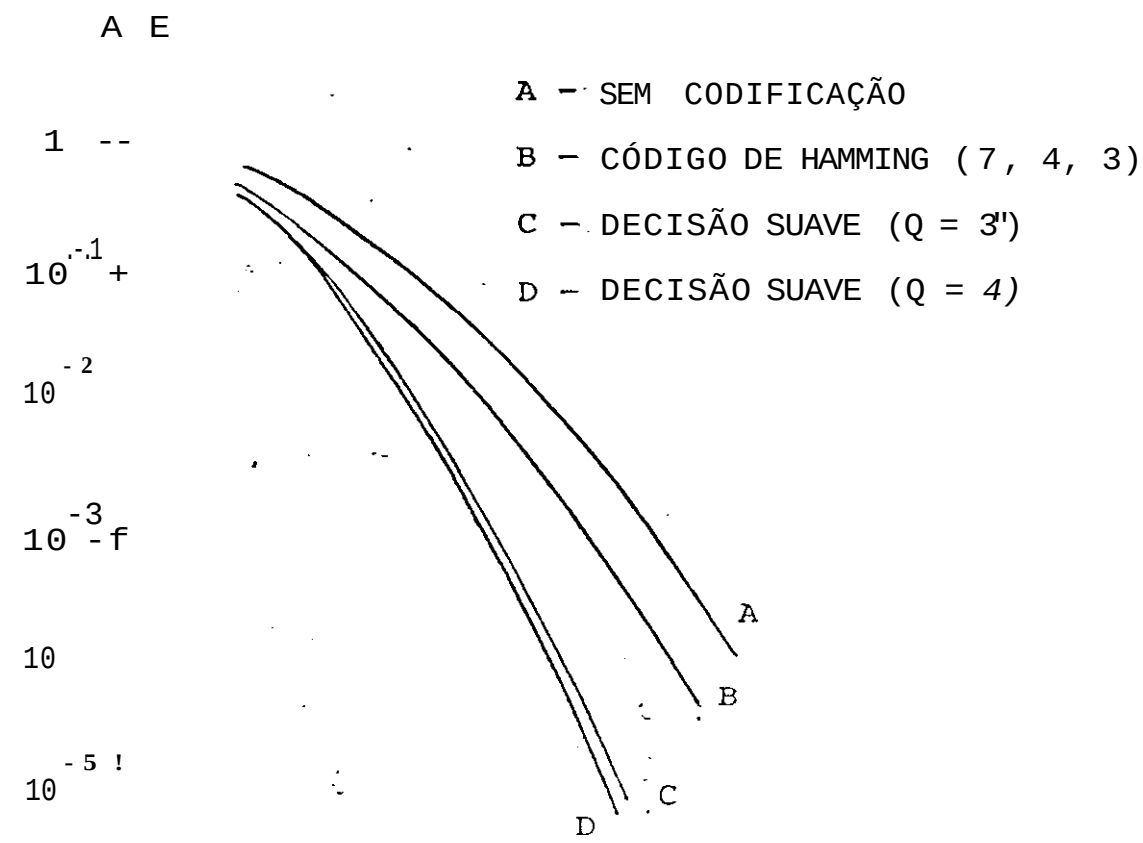


FIG. 4.17 - DETEÇAO POR ZONA NULA - SISTEMAS CODIFICADOS

4.5 - O ALGORtTMQ DE HARTMANN E RUDQLPH.

Hartmann e Rudolph^[3]^ introduziram um algoritmo de decodificaçao que ê ótimo no sentido de que minimiza a probabilidade de erro por símbolo para palavras [1] código eguiprováveis, em um canal binário simétrico, sendo exaustivo no sentido de que toda palavra do código dual é usada no processo de decodificação. Para um código de bloco linear C(n,k,d), o código dual e $C^{1}(n,n-k,d^{1})$, de modo que esta última característica torna-o bastante prático para códigos de alta eficiência, ao contrário do que acontece nas técnicas convencionais de códigos lineares. O algoritmo, descrito a seguir, é essencialmente estatístico sendo aplicável a códigos de bloco e códigos convolucionais.

Seja $c=(c_{0},c^{\wedge},....c_{n\_1})$ uma palavra de um código de bloco linear C(n,k,d) e c! = [1] = (c c],....,c. ') . a j-ésima palavra do código dual [1] C' (n,n-k,d^{1}) - A palavra c é transmitida através de um canal discreto sem memória cujo alfabeto de saída ê B, de modo que a palavra recebida ê $r = (r_{0},r^{\wedge},...r_{n-1})$ / ^eB. A questão que o algoritmo se propõe a resolver é, dado r, calcular uma estimativa c_m do dígito c_m EC, de modo que a [1] probabilidade de que $= c^{\wedge}$ seja máxima. Isto pode ser [1] feito se mostrarmos-que

$$P(c = s[r] = a\ A^{\wedge}Cs), \text{ o cte} \qquad (4.60)$$

e estimarmos $c_m = s$ como sendo o valor que maximiza $A(s)_m$ ^

O lado esquerdo de (4.6Q} e dado por

$$P_j-Cc^slr] = £ ^PCc|r\}$$ (4.61)

•ctC, c_m =s

ou

$$P_rCc_m=sIr) = £ P(r|c)(P(c)/P(r)3$$ (4.62)

CEC.,C $_m$=S

Considerando que os símbolos de C são elementos de GF(p) então tem—se

$$P(c) = \frac{}{P^k}$$ (4.63)

e (4.62) pode ser reescrita como

$$P(c_m=s|r) = -\frac{ÍLÍ}{PCr)} £ P(r|c)_{6o>(c_c}-_m$$ (4.64)

CEC

onde

$$^8« = \begin{cases} 1, & \text{se } t = j \\ 0, & \text{em caso contrario} \end{cases}$$

$$e_m - £(6_{mo'}/6_{ml'}.......6_{m(n-l)},)$$

Pode—se mostrar que (4-1) -

P-l

(4.65)

t=0

U . C

C4.66)

onde

F(r,u) = Y, p(r|vî w -U. V (4.67)
veV n

w = e-' representa a p—ésima_raiz com - plexa da unidade.-Substituindo Ç4.65) e (4.66) em (4.64) e le vando em conta que (apêndice A)

v.c p, se v E c

0 , em caso contrario

ceC

chegamos a

n-k
-n-1 P-l -st
P(c=s]r)=-P P(r) !● Z F^'c j "te m) (4.68)
m
t=0

Para canais sem memória, (4.67) pode ser reescrita como

n-1 n-1 p-l -iu
F(r,u) I I P(r |v^w 1 1 -TT ^PÍrjDw
n £=0 i=0 (4.69)

Ficamos então com

n-k
w -st
P(rí t=0 Z
j=l
rn-1 p-l
TT I * ‖ 1 /\ (4.70)
. £=0 i=0

e assim

$$ {}^{PCC}m^{=?}|^{rí} = \frac{-n-1}{pCr)} \hat{m}^{Csl} * "Sn\hat{} \quad C4.71) $$

rti I m m

No caso binãrio, i.e. quando p=2, o procedimento para de-codificação consiste em escolher

0, se A (0)>A (1)

1, em caso contrario

Esta forma comparativa da regra de decisão pode ser apresentada de maneira mais conveniente, com o uso do conceito de razão de semelhança. Nesse caso vamos ter(38)

^n—k , ~

e*=-0-'se I TT(TTT'

0=1 -£=0 \1 +

c_m = 1, em caso contrario

onde

P(r£|l)

representa a razão "de semelhança e $c^1.\hat{}$ é um elemento do código do dual £n,n—k,d'} cujo significado ê esclarecido no exem - pio a seguir.

Usaremos o código de Hamming (7,4) para [1] exemplificar a regra de decodificação, que neste caso torna - se:

QQ

escolher c_Q - 0 se $1 - \bullet_f \backslash "5^* > 0$ l + $

e CQ = 1 &ᵐ caso contrário.

Para este código, a matriz de teste de paridade e seu espaço-linha são:

$$tH3 = \left[\begin{array}{ccccccc|c} 1&1&1&0&1&0&0 & (a)\\ 0&1&1&1&0&1&0 & (b)\\ 0&0&1&1&1&0&1 & (c) \end{array}\right]$$

C ($cl_£$) :

c_0	c_l	c_2	c_3	Cl»	c_5		
0	0	0	0	0	0	0	
1	1	1	•0	1	0	0	(a)
0	1	1	1	0	1	0	(b)
1	0	0	1	1	1	0	(a)®(b)
0	0	1	1	1	0	1	(c)
1	1	0	1	0	0	1	(a)©(c) i.
0	1	0	0	1	1	1	(b)®(c) ;
1	0	1	0	0	1	1	(a)©(b)©(c)'

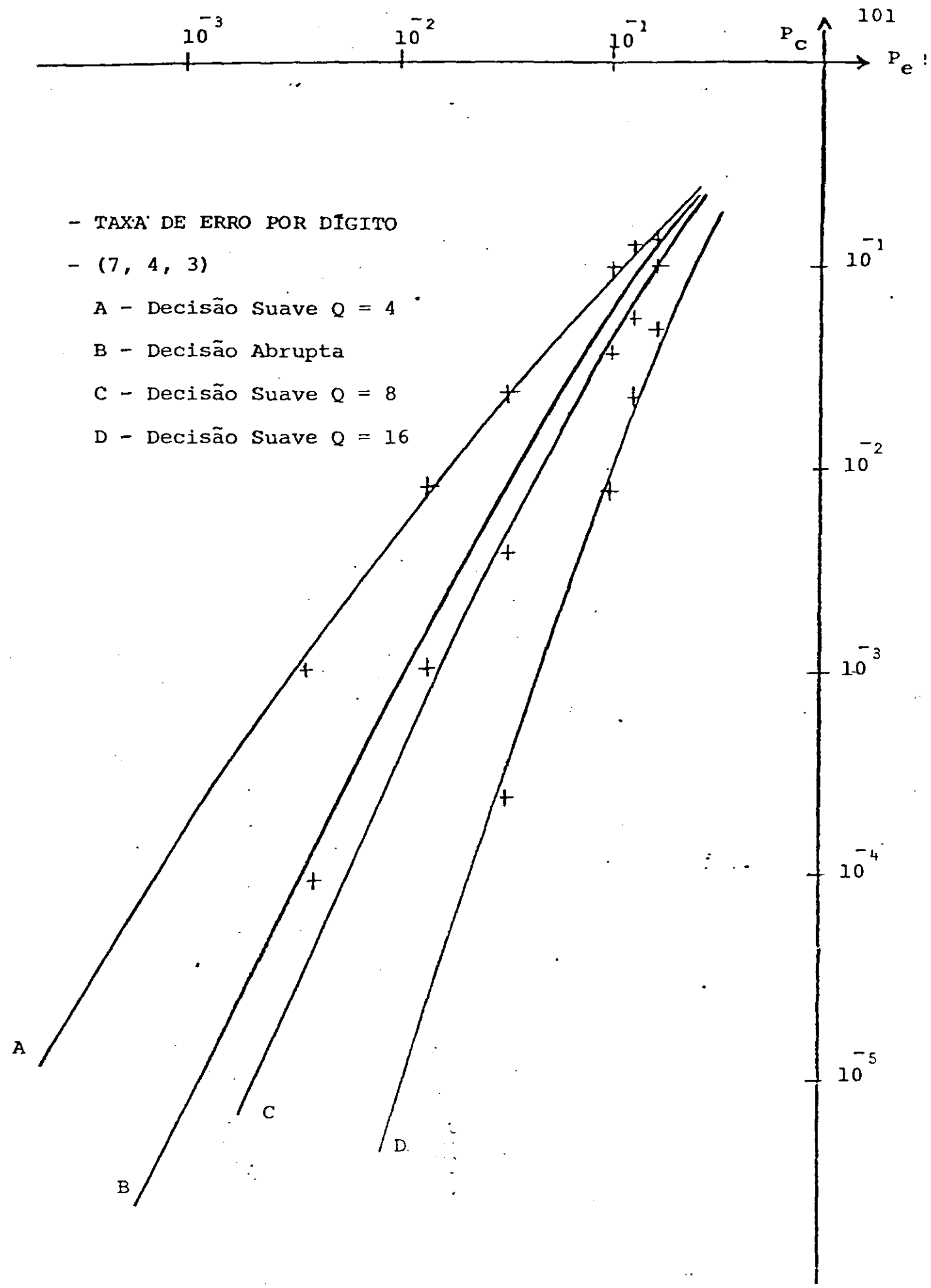
-fazendo $\frac{1 - }{1 + \text{⏢}} = p$, teremos

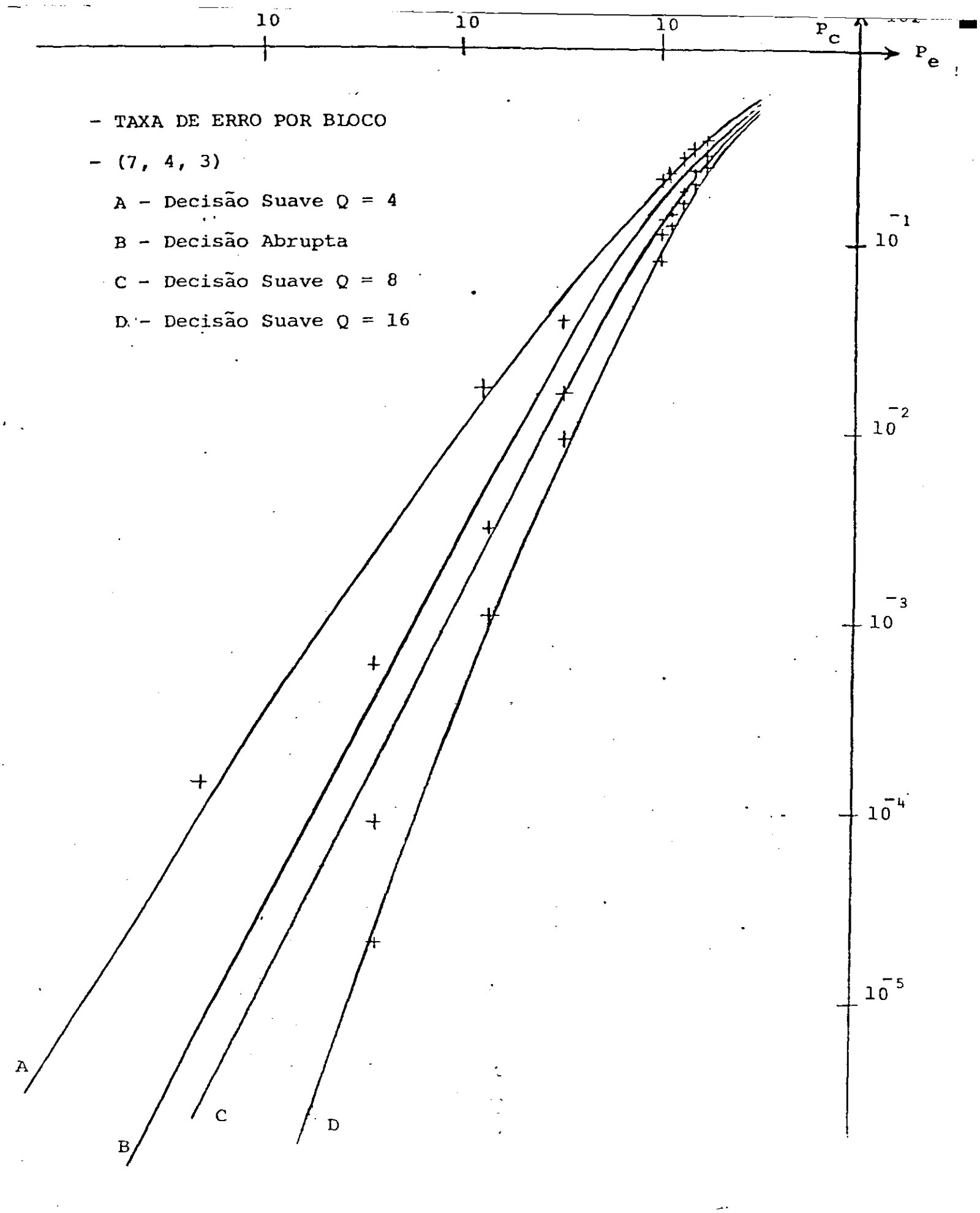
$c_0 = 0$ se $\text{£}_{PQ}{}^{8}{}' \; c\backslash_0 + 6_{00} \; x \; P \; P2 \; C\backslash_2 + <5_{,2} \; x \; p3 \; C\wedge 3 + 6003 \; x \; C\backslash_k + "SOM \; x \; P5 \; c\wedge_5 + {}^{6}05 \; x \; Pb \; c' + «DG \; i > 0$

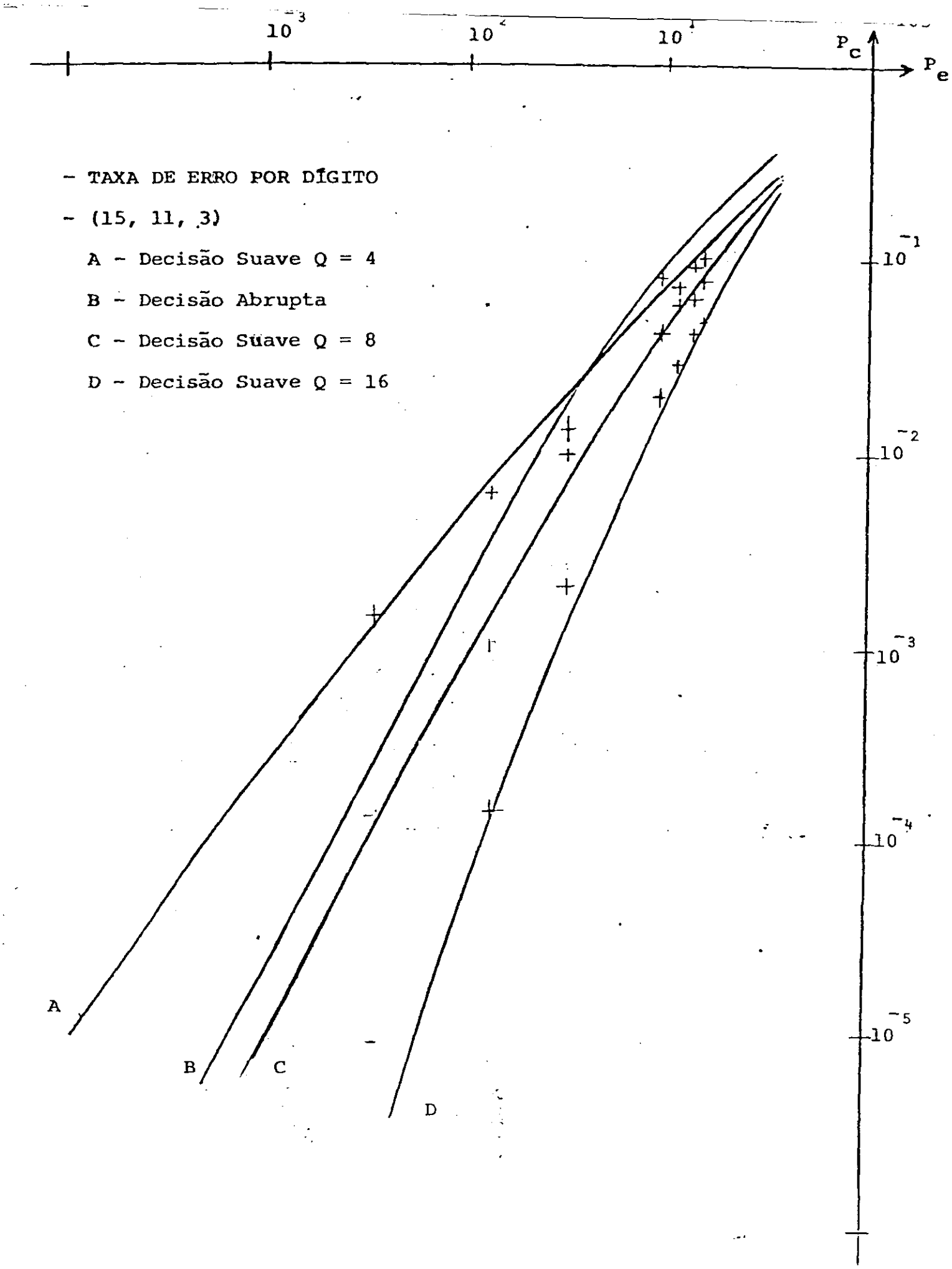
ou seja

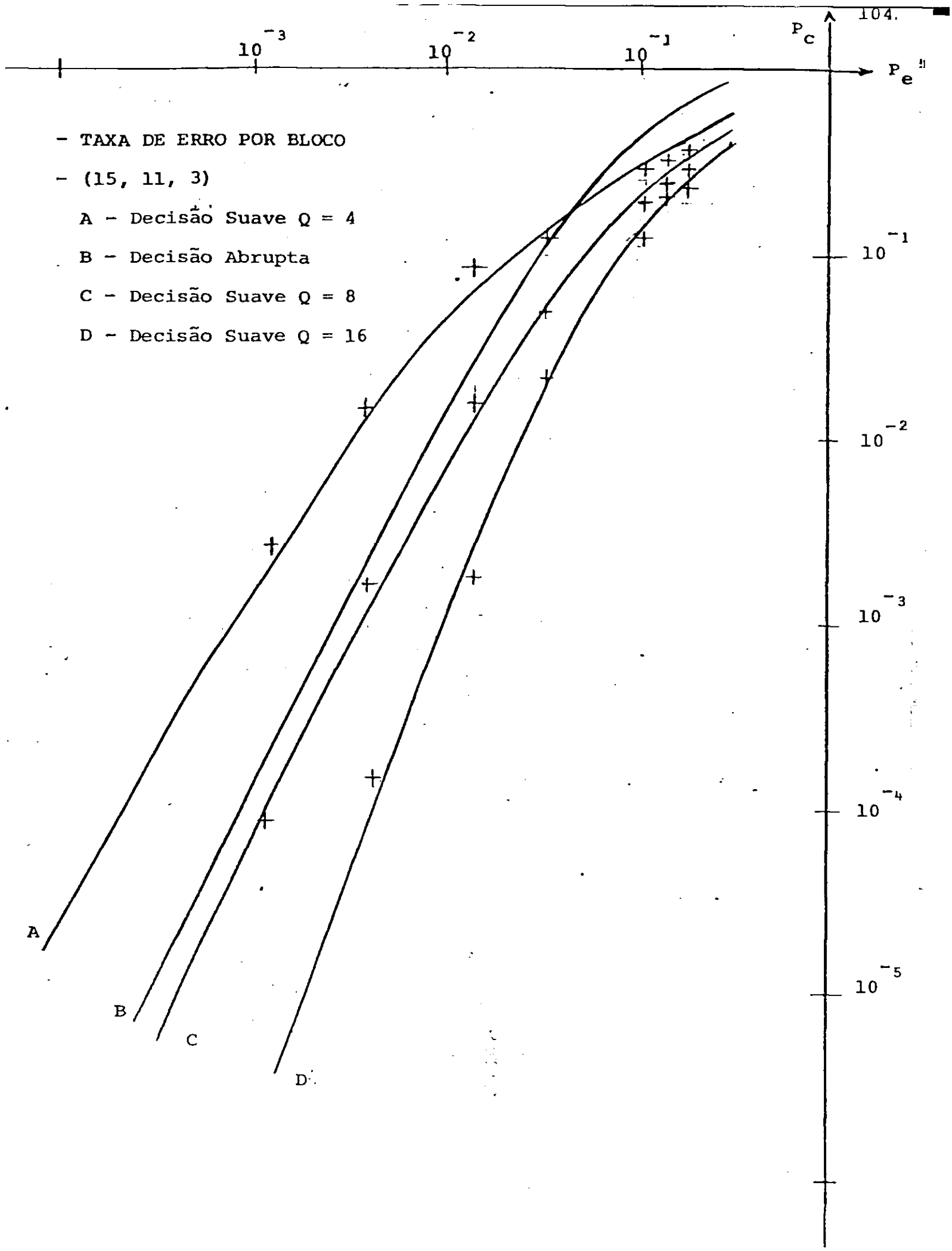
$c_Q = 0$ se $pQ + PjP\wedge P\wedge + P_{,}P_{3}P_{6} + P2P5{}^{p}6 + P_{3}{}^{p}\wedge{}^{p}5 + {}^{+} PQ{}^{p}1{}^{p}2{}^{p}3{}^{p}5 + {}^{p}0{}^{p}2{}^{p}3{}^{p}i,{}^{p}_{6} + {}^{p}0{}^{p}_{3}{}^{p},{}^{p}5{}^{p}6 \; °$

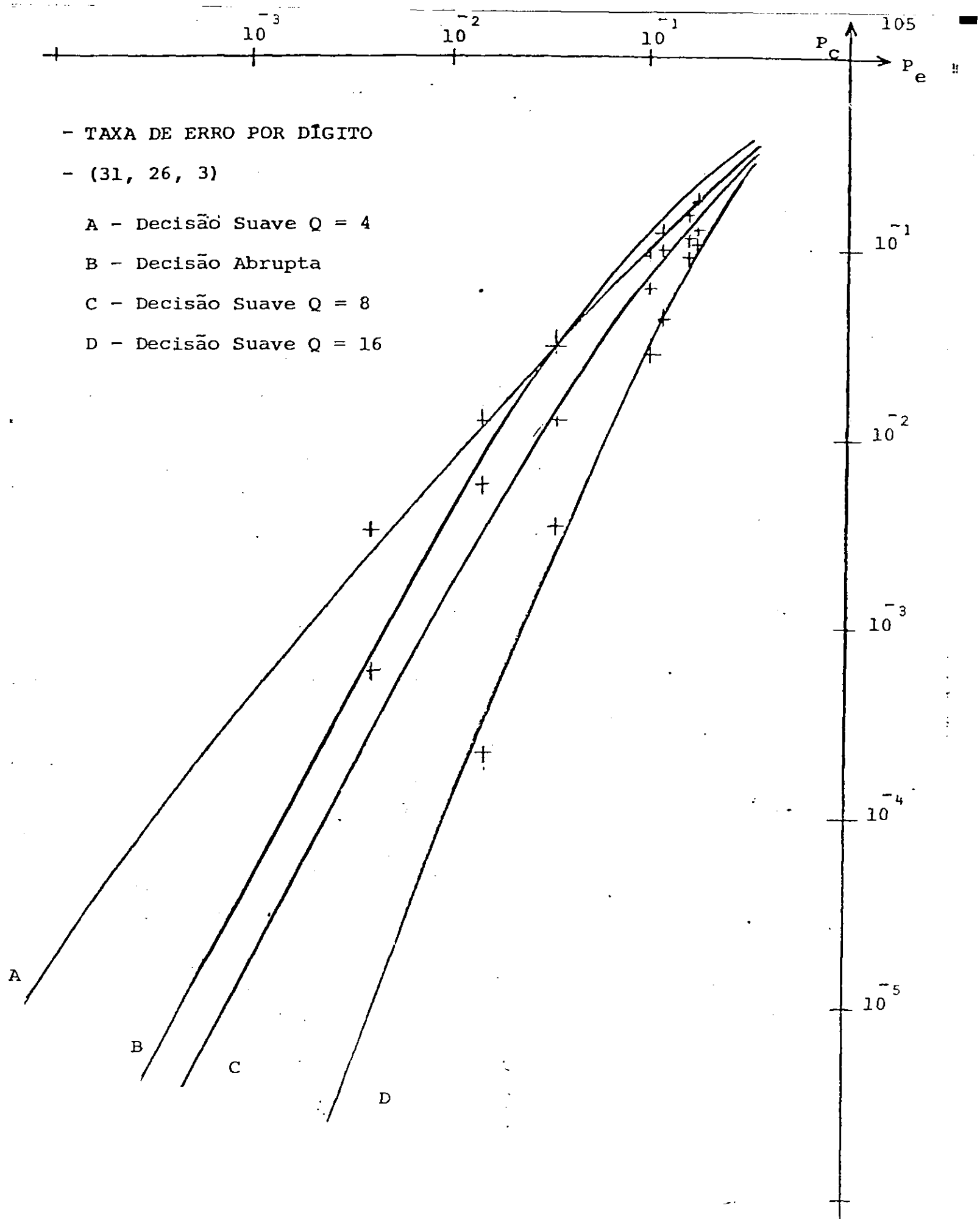
Testados o algoritmo de Hartmann e Rudolpb-, através. 3e simulação, em computador (Apêndice BJ , para alguns códigos de bloco lineares. Os gráficos obtidos estão mostrados nas ;pãginas 101 -a 112 . Foram usados três códigos cíclicos (7#4J, (15,11] e (31,26), todos com a mesma capacidade de correção. No capitulo seguinte é feita uma analise [1] desses resultados.

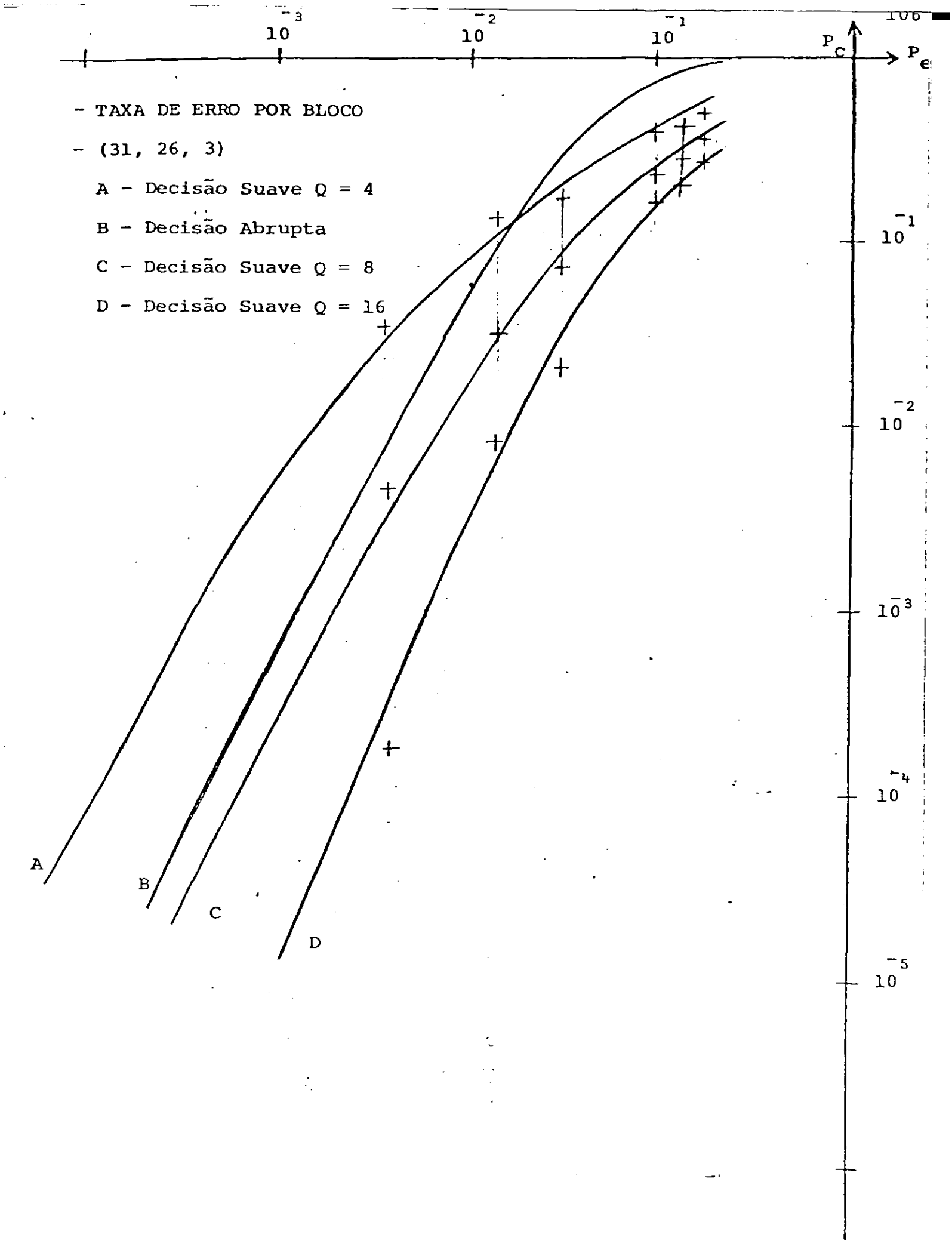

- TAXA DE ERRO POR DÍGITO
- (7, 4, 3)
A - Decisão Suave Q = 4
B - Decisão Abrupta
C - Decisão Suave Q = 8
D - Decisão Suave Q = 16
10^{-3}
10^{-2}
10^{-1}
P_c
101
P_e
10^{-1}
10^{-2}
10^{-3}
10^{-4}
10^{-5}
A
B
C
D

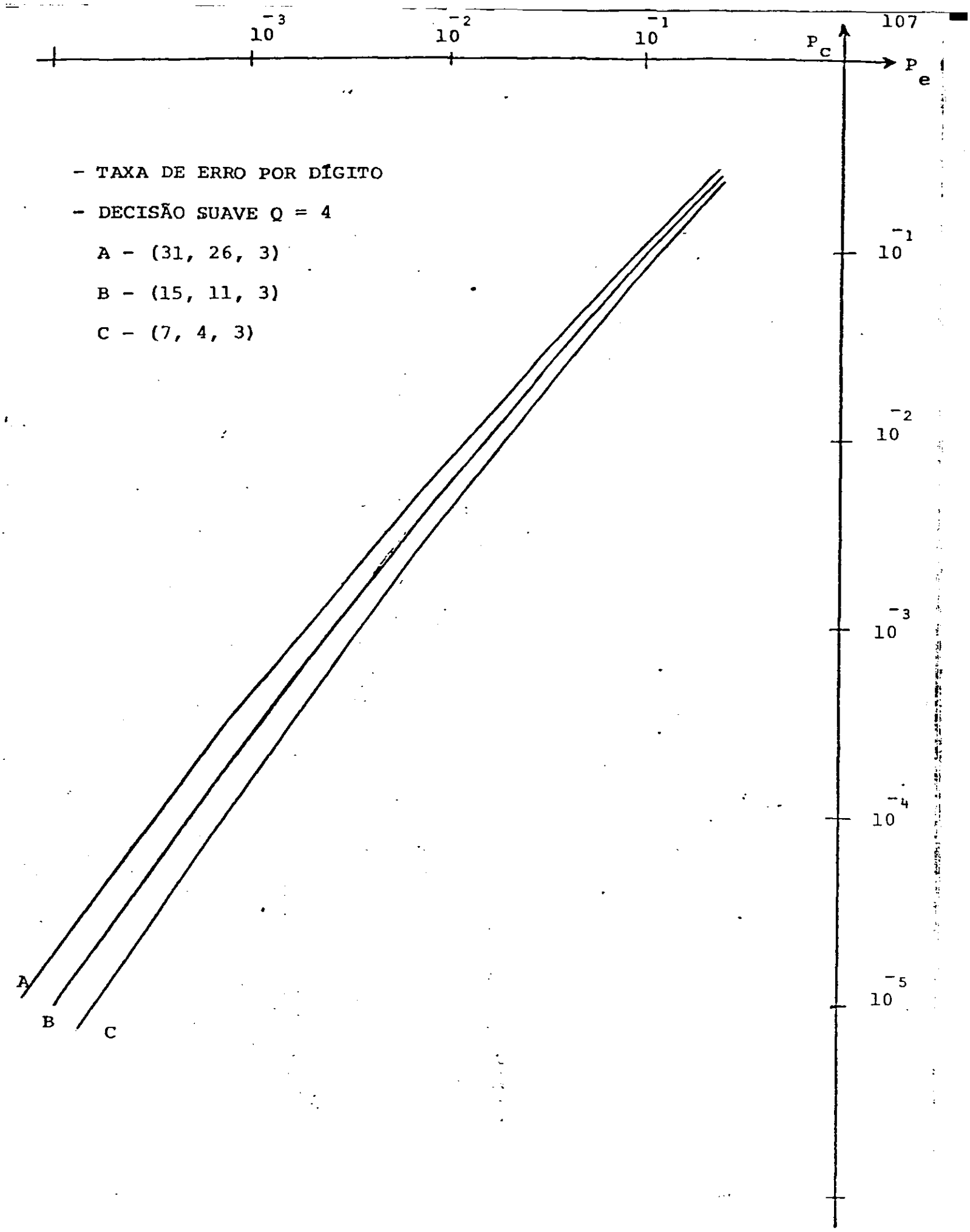

10
10
10
P_c
P_e
- TAXA DE ERRO POR BLOCO
- (7, 4, 3)
A - Decisão Suave Q = 4
B - Decisão Abrupta
C - Decisão Suave Q = 8
D - Decisão Suave Q = 16
10^{-1}
10^{-2}
10^{-3}
10^{-4}
10^{-5}
A
B
C
D

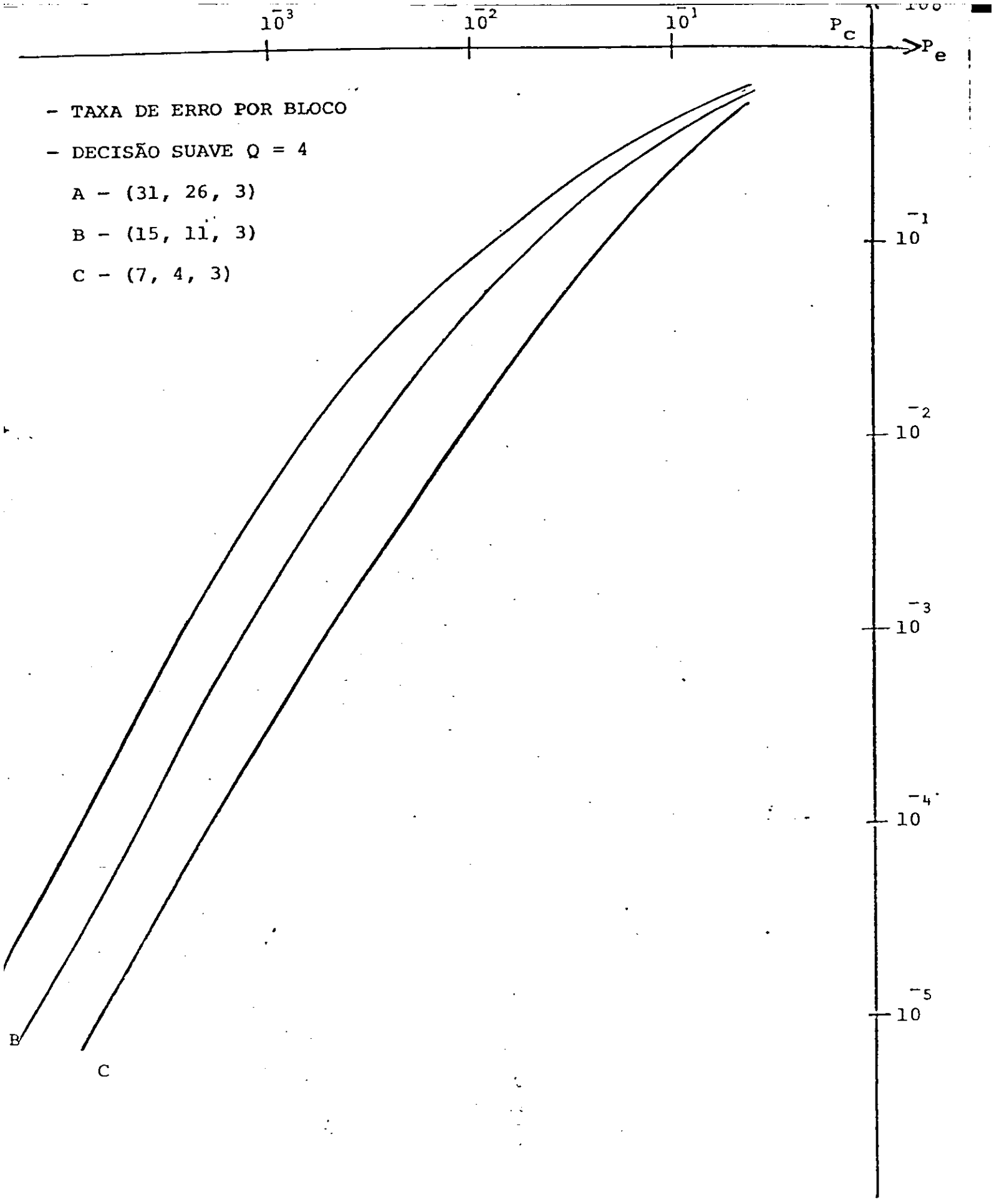

10^{-3}
10^{-2}
10^{-1}
P_c
P_e
- TAXA DE ERRO POR DÍGITO
- (15, 11, 3)
A - Decisão Suave Q = 4
B - Decisão Abrupta
C - Decisão Suave Q = 8
D - Decisão Suave Q = 16
10^{-1}
10^{-2}
10^{-3}
10^{-4}
10^{-5}
A
B
C
D

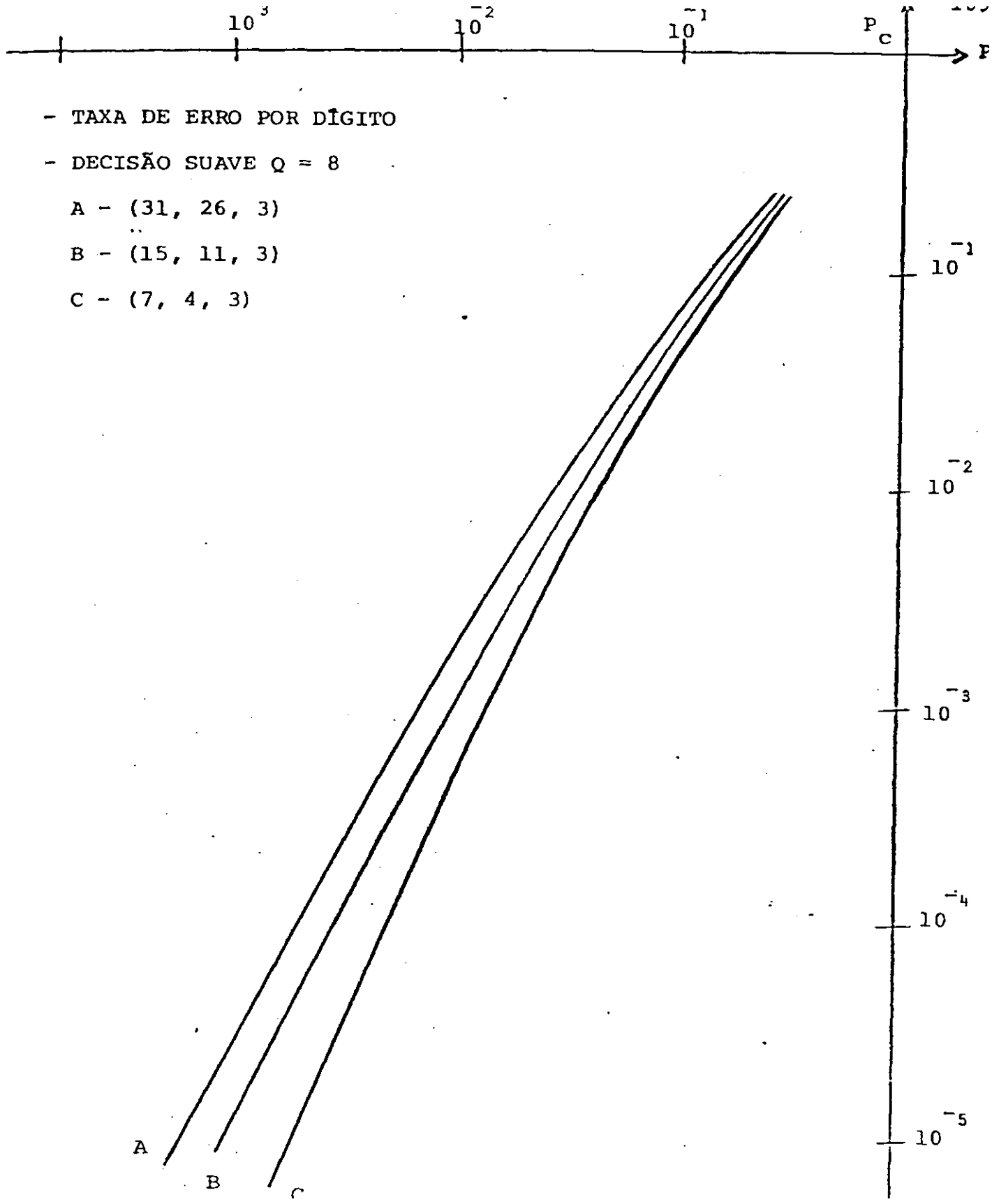

- TAXA DE ERRO POR BLOCO
- (15, 11, 3)
A - Decisão Suave Q = 4
B - Decisão Abrupta
C - Decisão Suave Q = 8
D - Decisão Suave Q = 16
10^{-3}
10^{-2}
10^{-1}
P_c
P_e
10^{-1}
10^{-2}
10^{-3}
10^{-4}
10^{-5}
A
B
C
D

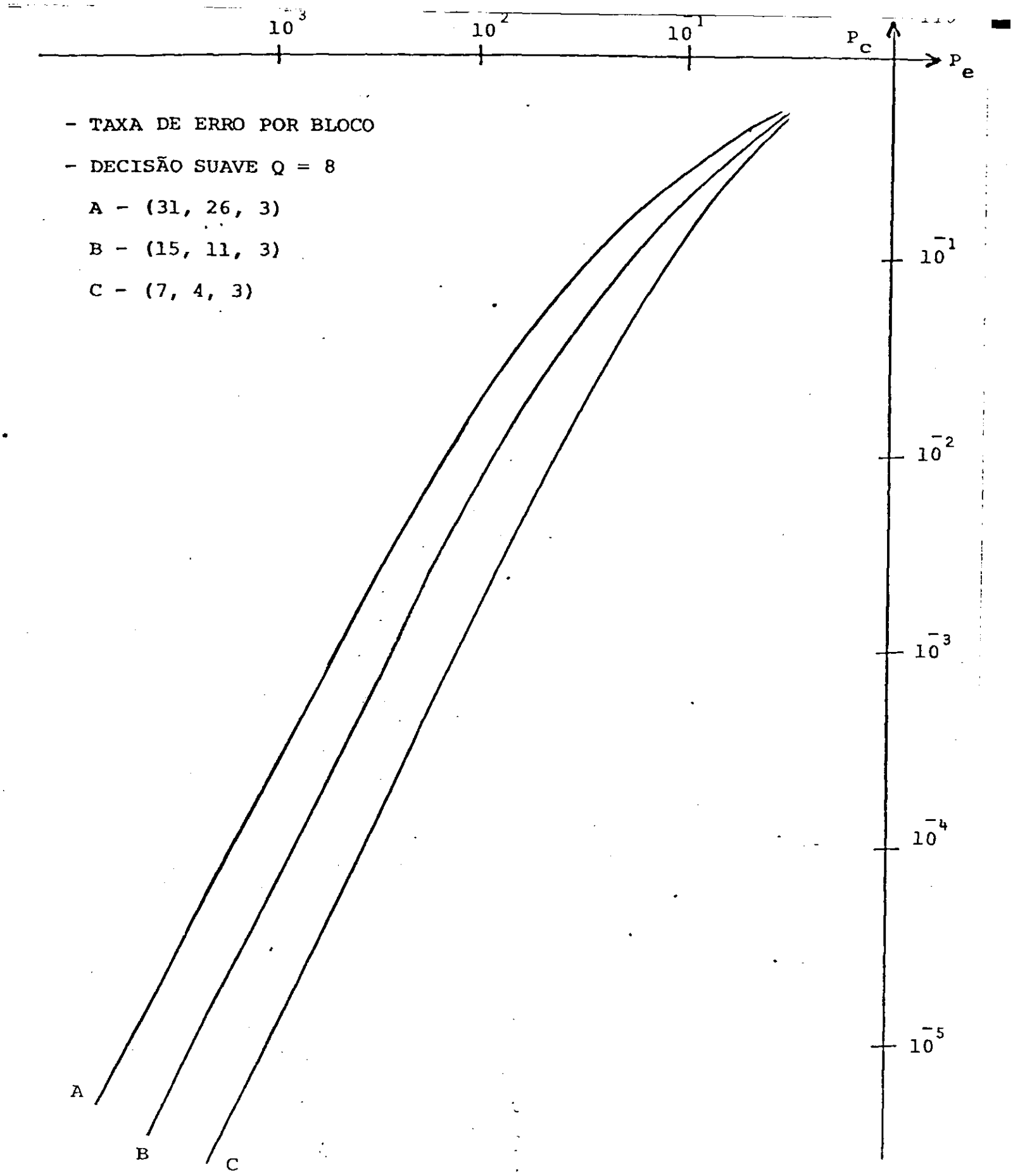

10^{-3}
10^{-2}
10^{-1}
P_c
105
P_e
- TAXA DE ERRO POR DÍGITO
- (31, 26, 3)
A - Decisão Suave Q = 4
B - Decisão Abrupta
C - Decisão Suave Q = 8
D - Decisão Suave Q = 16
10^{-1}
10^{-2}
10^{-3}
10^{-4}
10^{-5}
A
B
C
D

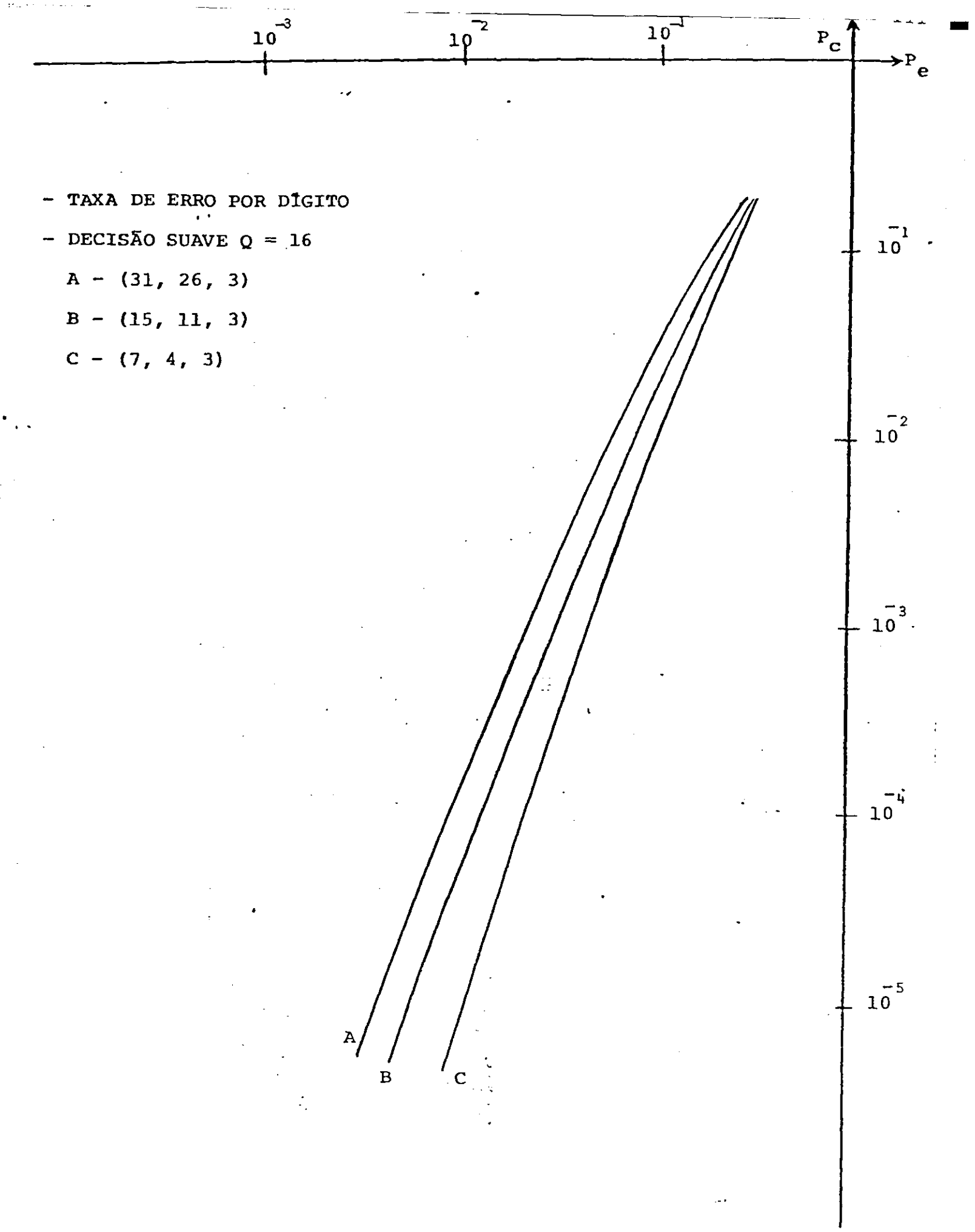

10^{-3}
10^{-2}
10^{-1}
P_c
P_e
- TAXA DE ERRO POR BLOCO
- (31, 26, 3)
A - Decisão Suave Q = 4
B - Decisão Abrupta
C - Decisão Suave Q = 8
D - Decisão Suave Q = 16
10^{-1}
10^{-2}
10^{-3}
10^{-4}
10^{-5}
A
B
C
D


10^{-3}
10^{-2}
10^{-1}
P_c
107
P_e
- TAXA DE ERRO POR DÍGITO
- DECISÃO SUAVE Q = 4
A - (31, 26, 3)
B - (15, 11, 3)
C - (7, 4, 3)
10^{-1}
10^{-2}
10^{-3}
10^{-4}
10^{-5}
A
B
C


10^{-3}
10^{-2}
10^{-1}
P_c
P_e
- TAXA DE ERRO POR BLOCO
- DECISÃO SUAVE Q = 4
A - (31, 26, 3)
B - (15, 11, 3)
C - (7, 4, 3)
10^{-1}
10^{-2}
10^{-3}
10^{-4}
10^{-5}
B
C


10^{-3}
10^{-2}
10^{-1}
P_c
P
- TAXA DE ERRO POR DÍGITO
- DECISÃO SUAVE Q = 8
A - (31, 26, 3)
B - (15, 11, 3)
C - (7, 4, 3)
10^{-1}
10^{-2}
10^{-3}
10^{-4}
10^{-5}
A
B
C


10^{3}
10^{2}
10^{1}
P_c
P_e
- TAXA DE ERRO POR BLOCO
- DECISÃO SUAVE Q = 8
A - (31, 26, 3)
B - (15, 11, 3)
C - (7, 4, 3)
10^{-1}
10^{-2}
10^{-3}
10^{-4}
10^{-5}
A
B
C

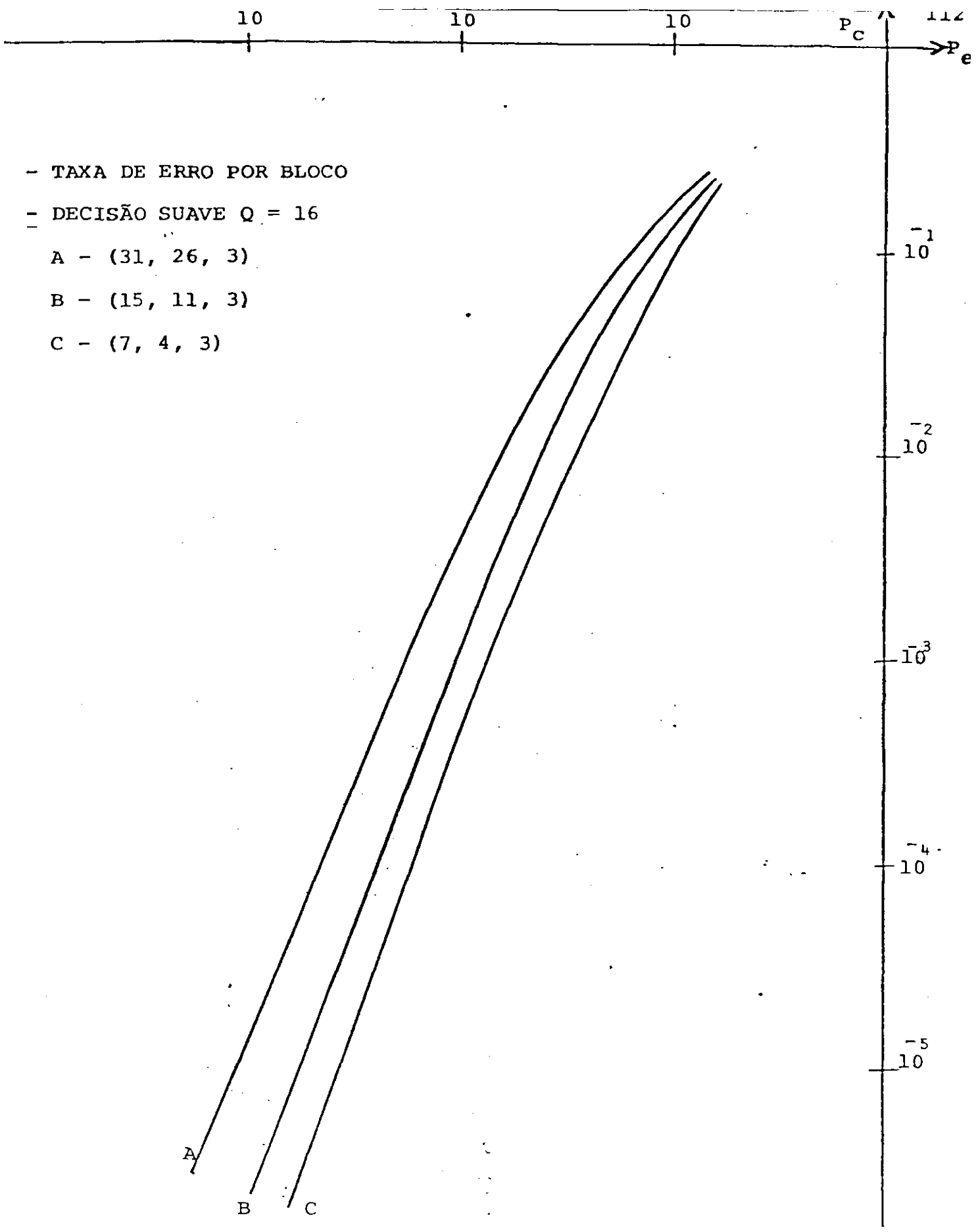


- TAXA DE ERRO POR DÍGITO
- DECISÃO SUAVE Q = 16

  A - (31, 26, 3)

  B - (15, 11, 3)

  C - (7, 4, 3)



- TAXA DE ERRO POR BLOCO
- DECISÃO SUAVE Q = 16

  A - (31, 26, 3)

  B - (15, 11, 3)

  C - (7, 4, 3)

CAPÍTULO V

C O N C L U S Õ E S

Neste capítulo analisamos os resultados obtidos na simulação do algoritmo de Hartmann e Rudolph , comparando e discutindo o desempenho e a complexidade do mesmo em relação aos procedimentos que não empregam decisão suave-

5.1 - ANALISE DOS RESULTADOS

Os gráficos das paginas.101 a 106 apresentam as curvas de probabilidade de erro na saída do decodificador ($p_{„}$) em função da probabilidade de erro no canal (p_e) para três códigos de bloco cíclicos. Em cada gráfico, as curvas representam um mesmo código, para três valores diferentes de regiões de quantização (Q) . Para efeito de comparação, mostramos também a curva obtida pelas técnicas convencionais' de decodiíicação.de códigos cíclicos[22]. Observamos que, tanto para probabilidade de erro por dígito, como para probabilidade de erro por bloco, o algoritmo de Hartmann e Rudolph [1] apresenta um desempenho superior'-ao método que não emprega decisão suave, quando se usa um numero--de regiões de quantização superior a quatro. Esta diferença é mais pronunciada nas curvas de probabilidade de erro por dígito, uma vez que o algoritmo testado opera minimizando esta probabilidade. Quando'

Q vale quatro, o métgdo conyenciona.1 é sempre superior, uma vez que nesse caso pouca informação de confiabilidade sobre as amostras colhidas é utilizada no processo de decisão.

Os gráficos das páginas 107 a 112 apresentam as curvas de P_c em função de P_e de modo a permitir uma comparação entre códigos de diferentes comprimentos, para um mesmo valor de Q. Qualitativamente, o resultado obtido é equivalente aquele que se tem com o procedimento convencional, isto ê, os códigos de menor-comprimento apresentam um desempenho melhor- Isto ê verdadeiro para todos os valores de Q testados.

5.2 - COMENTÁRIOS.

A técnica de decodificação de Hartmann e Rudolph ê ótima no sentido de minimizar a probabilidade de erro por dígito, para palavras código eguiprováveis transmiti, das através de um canal discreto sem memória, sendo aplicável a códigos lineares de bloco e convolucionais. Em relação a *este* critério seu desempenho ê superior aos procedimentos de de codificação, que são ótimos no sentido de minimizar a probabilidade de erro por palavra, isto é, a decodificação por correlação de códigos de bloco e o algoritmo de Viterbi para códigos convolucionais. Quando se compara a probabilidade de erro por palavra, o contrário acontece(38)

O principal mérito do procedimento de

Hartmann e Rudolph reside no fato de que para decodificar um código (n,k,d) , seu código dual (n/n-k/d¹). . é empregado . Isto faz com que esta seja, até agora, a única técnica conhecida viável para aplicação com códigos de alta eficiência.

A decodificaçao probabilística de códigos lineares tem ultimamente recebido maior ênfase na literatura sobre códigos corretores de erro, devido ã viabilidade de sua implementação prática por meio de microprocessadores- Massey. (39), mostrou que um demodulador de decisão abrupta ("hard decision") pode anular grande parte do ganho' que resulta da utilização de codificação de canal. Dessa forma esquemas de decisão suave, sempre que possível, devem ser empregados.

Como prosseguimento dos estudos desenvolvidos neste trabalho., sugerimos a investigação de esquemas de decisão suave que utilizem um posicionamento não uniforme das regiões de quantização, em função do tipo de ruído presente no sistema. Em relação ao algoritmo de Hartmann e Rudolph, uma extensão interessante seria a analise dos limites de desempenho do mesmo, principalmente em condições* de ruído adversas com taxas de erro próxijnas.: de 0,5. Sistemas deste tipo são de interesse para utilização em canais sujeitos a efeitos de- multipropagaçao e desvanecimento seletivo, -como ê o caso do canal de HF.

APÊNDICE A

ÁLGEBRA BÁSICA

A álgebra dos campos finitos desempenha[1] um papel extremamente importante na construção e implementação dos sistemas controladores de erros. Códigos que obedecem a uma estrutura algébrica bem definida apresentam duas características importantes; primeiro, suas propriedades são mais facilmente estabelecidas e, segundo, sua implementação é geralmente simples e prática, em comparação com outros tipos de códigos. Um exemplo marcante deste fato são os códigos BCH.

Neste-apêndice apresentamos alguns conceitos importantes para a teoria dos códigos de grupo, no sentido de dar ao leitor~a ferramenta matemática suficiente _ para a compreensão deste trabalho.

A . l GRUPOS

Os grupos tiveram a sua origem na teoria' das substituições devido, em parte, aos trabalhos de Lagran - ge^ . O verdadeiro iniciador deste capitulo da álgebra , no entanto, f o i o matemático francês-Evarist Galois(1812-1832) . O desenvolvimento da teoria dos gxupos era então condicionado por suas aplicações â teoria das equações algébricas. Mais ' tarde, os trabalhos de Sophus Lie (1842-1899)mostraram a iim - portância dos-grupos em certos aspectos das equações diferenci

ais, abrindo caminho pare, a teoria dos chamados grupos de Lie. A ampliação, do campo de aplicação dos grupos veio se dar com[1] os trabalhos de Felix Klein (1849-1925), que introduziu a ideia de se considerar a geometria como o estudo de proprieda des invariantes por grupos de transformações determinadas. Es sa idéia, introduzida em forma axiomática por Arthur Cayley [1] t.1821-1895) envolve dois aspectos: Os grupos aditivos e os [1] grupos multiplicativos. Na verdade, os primeiros constituem , a menos da notação, um caso particular destes últimos, de for ma que neste apêndice, vamos usar somente a notação referente aos grupos multiplicativos.

DEFINIÇÃO A.1.1

Um conjunto de objetos G, para os quais esta definida uma operação, que denotaremos por *, é um **GRUPO,** se satisfaz os seguintes axiomas:

1 - Para quaisquer elementos a e b e G, o elemento a * b e G.

2 - Para quaisquer três elementos a, b e c e G, tem-se

$$a * (b * c) = (a * b) * c = a * b * c.$$

3 – Existe no conjunto um e sõ um elemento n, tal que

$$n * a = a * n = a , \forall a \in G ; \quad -$$

n é chamado elemento neutro ^ou identidade) do grupo. No caso da adição e multiplicação usuais, temos n = 0 e n = 1, res - pectivamente.

4 – Todo elemento a do grupo possui um e sõ um inverso, que

representaremos por **i-** 0 elemento inverso é definido por **a * i = i * a —** n. No caso da adição e multiplicação usuais temos **i = —a** e **i = a** respectivamente.

O grupo que, além de satisfazer os axio - mas 1 a 4, satisfaz a propriedade comutativa, isto é,

a * b = b * a, Y a, b e G,

é chamado grupo Abeliano ou Comutativo. Neste apêndice lidare mos apenas com grupos^Abel-ianosVejamos - alguns exemplos.

EXEMPLO 1 - O conjunto dos números inteiros e um grupo Abelia no em relação â operação de adição.

EXEMPLO 2 - O conjuntordas matrizes quadradas-é" um grupo em relação ã operação-de multiplicação de matrizes. Note que es- te grupo não é Abeliano.

EXEMPLO 3 - Dado _um inteiro p > 1, consideremos_o_ conjunto G(p) formado pelos inteiros 0,1,...,p-1. Notemos, desde já que este conjunto não forma um grupo aditivo em relação ã operação de adição usual entre inteiros, uma vez que a soma de dois de seus elementos pode ser maior que (p-1). Entretan- to, é possível definir uma operação em relação .à qual G(p) é um grupo aditivo. Assim, se a e be G(p), definimos a soma mõ dulo p entre a e b como sendo~~D--resto~da divisão por p da adição usual (a+b). Como todo resto de uma divisão por p é igual a um dos inteiros de G(p), vemos que a adição mõdu lo p verifica o primeiro axioma dos grupos aditivos. Os

três axiomas restantes podem ser facilmente verificados, de modo que o conjunto G(pl juntamente com a operação adição modulo p forma um grupo aditivo, o qual também ê Abeliano.

Os grupos formam a estrutura mais simples na álgebra dos campos finitos. Sobre eles gostaríamos de observar ainda a existência de grupos de um ou dois elemen - tos. No primeiro caso, este elemento deve ser o elemento neutro n, enquanto que no segundo, os membros do grupo devem ' ser n e a; desde que J/a" precisa ter um inverso

$$a + n = a \quad /\ n$$

então

$$a + a = 0$$

ou

$$a = '-a.$$

Assim, a tabela de adição para este grupo apresenta-se como

+	0	a
0	0	a
a	a	0

O conjunto {0,a}, juntamente—com a tabela-de_adição acima satisfaz os axiomas 1 a 4, sendo portanto um grupo. Como a operação, definida é comutativa, istoe, 3 + 0 = 0 + 3 = a, o grupo é Abeliano.

Um grupo G pode ter um número finito ou infinito de elementos. No primeiro caso, G e chamado grupo finito e o número de elemento de G é a ordem do grupo. No exemplo dado anteriormente, G é um grupo de ordem 2.

A.2 CAMPOS

DEFINIÇÃO A.2.1 - Consideremos um conjunto F de elementos, sobre os quais estão definidos duas operações: "+"(adição) e "." (multiplicação). A operação adição associa a cada par a,b E F, um elemento (a+b)e F e a operação multiplicação associa' a cada par de elementos a,b e F, um elemento a,b £ F. O conjunto F é um campo se e somente se as duas operações definidas acima satisfazem as seguintes propriedades:

1 - A adição é comutativa, ou seja,

$$a + b = b + a, \quad V\ a\ \#\ b.-.e.F$$

2 - A adição é associativa, ou seja,

$$a + (b+c) = (a+b) + c = a + b + c, V\ a,b,c\ E\ F$$

3 - Existe um único elemento Ofzero") em F tal que

$$a + 0 = a, \quad V\ a\ e\ F$$

4 - Para cada a E-F, existe um e só um elemento (-a) e F, tal que

$$a + (-a) = Q$$

5 — A multiplicação é comutativa, isto é,

$$a.b = b.a, \ V^{a}/ \ E \ F$$

6 — A multiplicação é associativa, isto é,

$$a.(b.c) = (a.b).c = a.b.c, \ V \ a,b,c \ e \ F$$

7 - Existe um e só um elemento não nulo, denotado l(um), em F, talque

$$a.l = a, \ V^{a \ e \ F}$$

8 — A cada a E F nao nulo, corresponde um ünico a ^ E F, tal que

$$a.a^{-1} = 1$$

9 — A multiplicação ê distribuitiva em relação ã adição, ou seja,

$$a.(b+c) = a.b+a.c, \ V \ a,b,c \ E \ F$$

Vejamos alguns exemplos.

EXEMPLO 4 - 0 conjunto dos números reais (ou racionais, ou- complexos) é um campo em relação âs operações de adição e multiplicação da álgebra comum.

EXEMPLO 5 — O conjunto {0,1}, juntamente com as operações de

adição módulo **2** e multiplicação **modulo 2,** conforme mostra a tabela a, seguir, forma um campo de dois elementos.

+	0	1
0	0	1
1	1	0

	0	1
0	0	0
1	0	1

ADIÇÃO MODULO **2** MULTIPLICAÇÃO MODULO **2.**

Este campo é chamado campo de Galois de dois elementos e é representado por GF**(2) .**

Pode ser mostrado gue, para todo número p primo ou potência de um primo, existe um campo com p elemen tos^[1]^ - 0 conjunto de inteiros,modulo q, se q é primo, jun tamente com as operações de adição e multiplicação modulo q , forma o campo de Galois de q elementos, GF(q).

DEFINIÇÃO A.2.2 - Sejam F^ e dois campos e suponhamos que esta contido em F_2, isto e, F^ é um subconjunto de F_2. Então diz-se que F^ é um subcampo de F_2.

Assim, cada um dos campos que estivemos considerando ê um subcampo do campo dos números complexos. Em particular, podemos dizer que -R ê um subcampo de C, e Q ê um subcampo de R.

A.3 ESPAÇOS VETORXAIS

DEFINIÇÃO A.3,1 — Um conjunto V de elementos e unj espaço vetorial sobre um campo F, se ele satisfaz os seguintes axiomas:

1 - V é um grupo Abeliano em relação a operação de adição.

2 — Existe uma operação chamada multiplicação escalar, que **Y a e F e Y u e V** associa o elemento a u E V, a qual satisfaz as propriedades:

2.a - lu = u. "

2.b - $(a_1 a_2)u = a_1(a_2 u)$.

2.c - a(u + v) = a. u + a v.

2.d - $(a_1+a_2)u = a_1 u + a_2 u$.

Os elementos dos conjuntos V e F são chamados, respectivamente, —vetores e escalares. Vejamos alguns[1] exemplos.

EXEMPLO 6 - Consideremos o campo de Galois de dois elementos[1] GF(2) e seja* V_n o conjunto de todas as n-uplas

(v) = ' l ' 2 ' " * * * n J

de escalares -v_i c GF(2), isto ê,

v^ = 0,1 , i = 1,...n.

A soma-de duas~n—uplas Cu) e (v)

$$\mathbf{lul - Lu,,u_{0},...-u\ 1}$$

$$\mathbf{CvJ = Cv.}\ /\ V\ -\ ,\_\_\_\_\mathbf{v\ 3}$$
$$_{1}\quad _{z}\qquad\quad n$$

ê definida como sendo

$$\mathbf{(u) + [v]}\ -\ Cu.\ +\ \mathbf{v.},\ u\_\ +\ \mathbf{v_{„},....,u\ +v\ 3}$$
$$J\text{-}\quad x\quad \textit{£.}\quad \textit{2,}\qquad n\ n$$

onde $\mathbf{u_i + v._i}$ representa a soma modulo **2** entre $\mathbf{u}_i$ e $\mathbf{v}_i$. O produto de um escalar **c** de GF**(2)** por uma n-upla de V é de fdnido por

$$\mathbf{c\ Cv] = tc}\ v^{\wedge},\ c\ \mathbf{v}_{2},\ .\_\_\_,c\ V\ ]$$

onde **c.v^ representa a** multiplicação módulo **2** -de **c-** por **v^-**

É possível mostrar que as operações acima satisfazem os axiomas que definem um espaço vetorial sobre um campo ~F, de modo que o conjunto de todas as n-uplas b i - narias, juntamente com as operações de soma e multiplicação [1] modulo *2,* constitui um espaço vetorial sobre o campo GF**(2).**

DEFINIÇÃO A.**3.2** - Se V é um espaço vetorial sobre um campo[1] F, então um subconjunto W de V, que é um espaço vetorial [1] sobre F- com as operações de adição de vetores e multiplica- ção escalarí é um subespaço vetorial de V.

DEFINIÇÃO A.**3.3** - Seja V um espaço vetorial sobre um campo* F. Um vetor u e V é dito uma combinação linear dos K veto-

res ᵛi'ᵛ2'*"*ᵛ]tᴱ *V'* ᵃᵉ ^ ^ s t ^ escalares ᶜ*x*ᶜ*2'* °kᴱ ᶠ não todos nulos, tais que

$$u = \sum_{i=1}^{k} l_i \cdot x_i$$

EXEMPLO 7 - Sejam ᵛx'ᵛ2'"*""ᵛn ᵉˡᵉᵐᵉⁿᵗᵒˢᵈ o espaço vetorial V de todas as n-uplas sobre GF(2). Então o conjunto das combinações lineares do tipo

$$a_1 v_1 + a_2 v_2 + \ldots + a_n v_n$$

onde $a_i = 0,1$, é um subespaço W de V . Dizemos que W é o subespaço gerado pelos vetores •v^^,....v . Se ʷ~ᵛₙ' ᵒᵘ seja, se todo elemento de V_n e uma combinação linear dos V£/ -então dizemos que estes vetores geram o espaço V"ₙ sobre GF(2).

EXEMPLO 8 - Consideremos a matriz H de elementos em GF(2)

$$H = \left[\begin{array}{cccccc|c|c} 1 & 1 & 0 & 1 & 0 & 0 & & a \\ 1 & 1 & l_i & o & 1 & 0 & = & b \\ 0 & X & 1 & i & 0 & 1 & & c \end{array}\right]$$

O conjunto W formado por todas as combinações lineares dos vetores linhas a,b,c de A, constitui um subespaço do espa–

ço vetorial de todas as setuplas. Este subespaço ê chamado o espaço-linha de H.

DEFINIÇÃO A.3.4 - Seja V um espaço vetorial sobre um campo F. Um subconjunto S de V é dito linearmente dependente se existem vetores $v_1, v_2, \ldots, v_n$ em S e escalares $c_1, c_2, \ldots, c_n$ em F, não todos nulos, tais que

$$c_1 v_1 + c_2 v_2 + \ldots + c_n v_n = 0$$

Em caso contrario, S é dito linearmente independente.

DEFINIÇÃO A.3.5 - Uma base de um espaço vetorial V é um conjunto de vetores linearmente independentes em V que gera V. O numero de elementos de uma base de V é chamado a dimensão de V.

EXEMPLO 9 - Consideremos os vetores (n-uplas binarias) linearmente independentes v_1, v_2 e v_3

$$v_1 = (1\ 0\ 0\ 1\ 0\ 1\ 1)$$

$$v_2 = [\ 0\ 1\ 0\ 1\ 1\ 0\ 1\ ]$$

$$v_3 = [\ 0\ 0\ 1\ 0\ 1\ 1\ \ 1)$$

O conjunto formado por todas as combinações lineares de v_1, v_2, v_3 forma subespaço do espaço vetorial das setupias. Os elementos v_1, v_2, v_3 constituem uma base para este subespaço, o qual tem dimensão 3.

DEFINIÇÃO A. **3.6** - Seja V um espaço yetorial sobre o campo *F.* Um produto escalar sobre V ê uma regra .que a cada par u,v de elementos de V associa um escalar em F , indicado por * u.v . Paira u e v do tipo

Cu3 = Cu^,u₂,....,u)

(v) = Cv₁,v₂/_____,vₙD

o produto escalar e calculado por

Cu)„Cv] = u_1 v_1 + u_2 v_2 +....+ u_n v_n

Se

Cu] . Cv) = 0

então dizemos que as n-uplas Cu) e (v) são ortogonais.

Costuma—se representar por G^1 o conjun-

(19)

to de todos os elementos E V que são ortogonais a um subconjunto C de V. Pode-se mostrar que C^1 e um subespaço' de V, denominado o espaço ortogonal a C, e que os elementos de C são ortogonais a todas as combinações lineares dos elementos de C.

APÊNDICE B

PROGRAMA PE COMPUTADOR

```
C  DECODIFICAÇÃO DE CÓDIGOS LINEARES
C  ALGORITMO DE HARTMANN E RUDOLPH
   IMPLICIT REAL*4      (A-H, O-Z)
   INTEGER BIT, W, SM2
   DIMENSION 0(8,7), FF(8,7), T(7), R0(7), BEST(7), Yl{7)'
   DATA D/O., 1., 0., 1., 0., 1., 0., l.,'.0., 2*1., 2*0., 2*1.,
  2 2*0., 2*1., 0., 1., 2*0., 1., 2*0., 4*1., 3*0., 1., 0., 2*1.,
  2 0., 1., 3*0., 2*1., 2*0., 2*1., 4*0., 4*1./
   NC = 7
   KC = 4
   W = 8
   SQ2 = SQRT(2.)
   IX = 1
   IW = 9
   A = 10
   DO 50 NJ = 2,4'
   NQ -= 2.**NJ
   DO 45 N = 3,19,4
   SNR = FLOAT ( N - l )
   Z = 10.**(SNR/20)
   SIGMA = A/Z
   TBE = 0.
   TPE = 0.
   BIT = 10 ** 6
```

```
      B I = Z * CK + 11 / CNQ * .SQ21
      B2 = Z * K / CNQ * .SQ2]
      PO = 0-5 * CERFCB1) - ERPCB2H
      GO TO 7
6     B = Z / CNQ * SQ2)
      Pl = 0.5 * .11. + ERFÇB) ]
      B = Z * CNQ - 1) / CNQ * SQ2)
      PO = 0.5 * CERFC(B) )
7     T (I) = Pl / PO                    RAZÃO DE SEMELHANÇA
      R0(I) = CL - T(I)) / Cl. + TU ) )
10    CONTINUE
      IF (M.EQ.NC) GO TO 40
      SP = 0.                      ALGORITMO DE. HARTMANN E RUDOLPH
      DO 35 I = 1, NC
      DO 25 J = 1, W
      PROD =1
      DO 20 L = 1, NC
      DELTIL = 1
      I F ( I - L ) 11, 12, 11
11    DELTIL = 0    '
12    CONTINUE
      SM2 ~ 1
      IF (D(J,L)-DELTIL) 17, 15, 17
15    SM2 = 0
17    CONTINUE          "*                .
      FF (J,L]=R0(L) ** SM2
20    PROD = PROD * FF(J,L)
25    SP = PROD + SP
      BESTCD = 0.
```

```
DO 40 KDIG = 1, BIT, 7
BLOCO = 0.
M = 0
DO 10 I = 1, NC
CALL RANDU ( I X, I Y, YFL)  GERAÇÃO DE RUlDO GAUSSIANO
IX = IY
V I = 2*YFL - 1
CALL RANDU ( IW, I Z, ZFL)
IW = I Z
V2 = 2*ZFL - 1
S = Vl**2 + V2**2
I F (S - 1)57, 55, 55
V = V1*SQRT (-2*ALOG(S)/S)
Y = SIGMA * V
Y1(I) = Y
K = 0
K = K + 1
IF ( ( Y - A*K/NQ ). GT. 0. ) GO TO 2  REGIÕES DE QUANTJZAÇÃO
I F ( ( K - 1 ) . GT. 0.) GO TO 4
B = Z * (NQ - 1) / (NQ * SQ2)
Pl = 0.5 * ERFC(B)
B = Z/CNQ * SQ2)
PO = 0.5 * ( 1 . + ERFCB) )
M = M + K                                .;
GO TO 7
I F ( (K - NQ + 1) . GT. 0. ) GO TO 6
B l = 7 * CNQ - K) / (NQ * SQ2)
B2 = Z * (NQ - K - 1) / (NQ * SQ2)
Pl = 0.5 * (ERF(B l) - ERF(B2)J
```

```
      IF  ((SP).  GT-;  0.)  GO  TO  29
      BEST(I) = 1." '
   29 CONTINUE
      TBE = TBE + BEST ( I )
      BIOCO = BLOCO + BEST(I)
   35 CONTINUE
      PEST = 0 .
      IF (BLOCO) 38, 38, 36
   36 PEST = 1. *
   38 CONTINUE
      TPE = TPE + PEST
   40 CONTINUE
      PEB  =  TBE/BIT
      PEP = TPE * NC / B I T .  .
      WRITE ( 6 , 499) NQ, SNR, TBE, PEB, TPE, PEP
  499 FORMAT ( '0' , 4X,  *NQ =    14, 4X, 'SNR = ', E14.8, 4X,
     2   'TBE  =  ', E14.8,  4X,  'PEB  =  ', E14.8,  4X,  'TPE = ', E14.8,4X
     2   'PEP = ' , E14.8)
   45 CONTINUE
   50 CONTINUE
      STOP
      END
```

REFERENCXAS

1 - H.NYQUIST, "Certain Factors Affecting Telegraph Speed", Bell System Technical Journal (B.S„T.J), 3, N9 2, abril, 1924.

2 - N.WIENER, "The Extrapolation, Interpolation, and Smoothing of Stationary Time Series with Engineering Applications", Wiley, N.Y., 1949 (o trabalho original surgiu como um relatorio do MIT Radiation Laboratory, em 1942).

3 - CLAUDE E.SHANNON e W.WEAVER, "The Mathematical Theory of Communication", Universidade de Illinois, Urbana, 1949.

4 - Bell Telephone Laboratories, "Transmission Systems for Communications", 4- ed. Western Electric, North Carolina, 1971.

5 - W. R. BENNETT e J.R.DAVEY, "Data Transmisson", Mc Graw-Hill, New York, 1965.

6 - ROBERT G.GALLAGER, "Information Theory and Reliable Communication", John Wiley New York, 1968.

7 - N.ABRAMSON, "Information Theory and Coding", Mc Graw-Hill, New York, 1963.

8 - F-M.REZA, "An Introduction to Information Theory", Mc Graw-Hill,,^ew York, 1961.

9 - B.GOLDBERG, "Communications Channels: Characterization and Behavior", IEEE Press, New York, 1976.

10- J.L.MASSEY, "Threshold Decoding", The MIT Press, Cambridge, Massachusetts, 1963.

11- E.R.BERLEKAMP, "Algebraic Coding Theory", Mc Graw-Hill, New York, 1968.

12- J.M.WOZENCRAFT e B.REIFFEN, "Sequential Decoding", The Technology Press e John Wiley, New York, 1961.

13- A.J.VITERBI, "Error bounds for convolutional codes and an asymptotically optimum decoding algorithm", IEEE Trans. Info. Th.,. vol IT-13, abril 1967.

14- R.H.HAMMING, "Error Detecting and Error Correting Codes", B.S.T.J., 29, Abril, i!950.

15- R.C.BOSE e D.K. RAY—CHAUDHURI, "On a Class of Error Correcting Binary Group Codes", Information and Control, 3, 1960.

16- A.HOCQUENGHEM, "Codes Correcteurs d'erreurs", Chiffres, 2, 1959.

17 - P.ELIAS, "Coding for Noisy Channels", IRE Convention Record, Parte 4, 1955.

18 - W.W.PETERSON e E.J.WELDON Jr., "Error-Correcting Codes",The Mit Press, 2- ed., Massachusetts, 1972.

19 - K.HOFFMAN e R.KUNZE, "Linear Algebra", Prentice-Hall, New Jersey, 1961.

20 - P.G.FARREL, "A survey of Errol-Control Codes", The Univer - sity of Kent Press, Canterbury, 1977.

21 - E.PRANGE, "Cyclic Error-Correcting Codes in two Symbols" , AFCRC-TN-57, 103, Massachusetts, 1957.

22 - V.C.ROCHA Jr., "Versatile Error-Control Coding Systems" , Ph.D.Thesis, University of Kent at Canterbury, 1976.

23 - S.LIN, "An Introduction to Error-Correcting Codes",Prentice-Hall, New Jersey, 1970.

24 - J.E.MEGGITT, "Error Correcting Codes for Correcting bursts of Errors", IBM JOURNAL OF RESEARCH AND DEVELOPMENT, 4, ju - lho, 1960.

25 - L.D.RUDOLPH, "A Class of Majority Logic Decodable^Codes" , IEEE Trans. Info. Th., Vol. IT-13, abril 1967.

26- L..D.RUDOLPH e M.E-MITCHELL, "Implementation *of,* Decoders for Cyclic Codes[11], XEEE Trans. Info. Th., Vol. IT-10, Julho, 1964.

27- W.W.PETERSON, "Encoding and Error-Correction Procedures for the Bose-Chaudhuri Codes", IRE Trans. Info. Th., Vol. IT-16, setembro, 1960.

28- R.T.CHIEN , "Cyclic Decoding Procedure for the Bose-Chaudhuri-Hocquenghem Codes",. IEEE Trans. Info. Th., Vol. IT-10, outubro/ 1969.

29- E.R.BERLEKAMP, "On Decoding Binary Bose-Chaudhuri-Hocquenghem Codes", IEEE Trans. Info. Th., Vol. IT-11, outubro 1965.

30- J.L.MASSEY, "Step-by-Step Decoding of the Bose-Chaudhuri-Hocquenghem Codes", IEEE Transrlnfo. Th., Vol. IT-11, outubro, 1965.

31- J.M.WOZENCRAFT e I-M.JACOBS, "Principles of Communication Engineering", John Wiley, 1965.

32- J.H.VAN LINT, "Nonexistence Theorems for Perfect Error-Correcting Codes", Computers in Algebra and Number Theory, SIAM AMS Proc./Vol. 45, 1970..

33- N.KALLIGEROS, "Soft-Decision Error-Correction", M.Sc. Dissertation, University of Kent at Canterbury,-England, 1977.

34- M.SCHWARTZ, "Information Transmission, Modulation, and Noise"., Mc Graw-Kill, New York, 1970.

35- C.N.HARRISON, "Application of Soft Decision Techniques to Block Codes", Proc. 1ERE Conference on Digital Processing of Signals in Communications, Loughborough, England, N9 37, 1977.

36- P.G. FARREL, E.MUNDAY e N.KALLIGEROS, "Digital Communications Using Soft Decision Detection Techniques", University of Kent at Canterbury, England, 1978.

37- F.J.BLOOM et al, "Improvement of Binary Transmission by Null-Zone Reception", Proc. IRE, Vol. 45, 1957.

38- C.R.P.HARTMANN e L.D.RUDOLPH, "An Optimum Symbol-by-Symbol Decoding Rule for Linear Codes", IEEE Trans.Info.Th., Vol. IT-22, Setembro 1976.

39- J.L.MASSEY, "Coding and Modulation in Digital Communications", Proc. Zurich Int. Seminar on Digital Communications, 1974.

40- C.B.BOYER, "A History of Mathematics", John Wiley, New York, 1968.